Algorithms and Computation in Mathematics 30

Manuel Kauers

D-Finite Functions

Springer

Algorithms and Computation in Mathematics

Volume 30

With this forward-thinking series Springer recognizes that the prevailing trend in mathematical research towards algorithmic and constructive processes is one of long-term importance. This series is intended to further the development of computational and algorithmic mathematics. In particular, Algorithms and Computation in Mathematics emphasizes the computational aspects of algebraic geometry, number theory, combinatorics, commutative, non-commutative and differential algebra, geometric and algebraic topology, group theory, optimization, dynamical systems and Lie theory. Proposals or manuscripts that center on content in non-computational aspects of one of these fields will also be regarded if the presentation gives consideration to the contents' usefulness in algorithmic processes.

Manuel Kauers

D-Finite Functions

Springer

Manuel Kauers
Institute for Algebra
Johannes Kepler University of Linz
Linz, Austria

ISSN 1431-1550
Algorithms and Computation in Mathematics
ISBN 978-3-031-34651-4 ISBN 978-3-031-34652-1 (eBook)
https://doi.org/10.1007/978-3-031-34652-1

Mathematics Subject Classification: 05A15, 33F10, 68W30

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

A univariate function is called D-finite if it satisfies a linear differential equation with polynomial coefficients. The concept of D-finiteness applies more generally to sequences satisfying recurrences, to multivariate functions satisfying systems of differential equations and/or recurrences, and to other objects. D-finite functions play a central role in the part of computer algebra that provides algorithms for formal power series, special functions and sequences, and symbolic summation and integration, and these algorithms find applications in a large (and growing) variety of different areas in which D-finite functions arise naturally.

A considerable part of our knowledge about D-finite functions goes back to the nineteenth century and has since become part of the mathematical culture that is often taken for granted. As such, these ideas are not easily accessible to people entering the area. At the other end of the timeline, during the past few decades we have seen the number of new articles related to D-finite functions exploding, and this amount of information also makes it difficult for newcomers to find orientation in the area. My goal for this book was to provide a solid starting point for people who want to enter the subject. With a strong emphasis on computational aspects, the book develops the theory of D-finite functions starting from classical and "well-known" results and techniques all the way up to some fairly recent developments.

There is a close analogy between linear recurrence equations with polynomial coefficients and linear differential equations with polynomial coefficients, but there are some differences as well. Rather than jumping back and forth between these two main cases, I decided to first treat only the recurrence case (Chap. 2) and then repeat the same program for the differential case (Chap. 3). It is not necessary to read or teach the chapters in this order. In particular, it may be better to go through Sects. 3.4–3.6 before Sects. 2.4–2.6. Here is a summary of all the section dependencies in Chaps. 2 and 3:

$$
\begin{tikzcd}
\boxed{2.1} \arrow[r] \arrow[d] & \boxed{2.2} \arrow[r] \arrow[d] \arrow[rr, bend left] & \boxed{2.3} & \boxed{2.4} \arrow[r] & \boxed{2.5} \arrow[r] & \boxed{2.6} \\
\boxed{3.1} \arrow[r] & \boxed{3.2} \arrow[r] \arrow[rr, bend right] & \boxed{3.3} & \boxed{3.4} \arrow[r] & \boxed{3.5} \arrow[r] & \boxed{3.6}
\end{tikzcd}
$$

In Chap. 4, we merge the two parallel threads of Chaps. 2 and 3 and continue the discussion in the language of operators, which besides the recurrence case and the differential case also covers some further situations. Although Chap. 4 occasionally uses results of Chaps. 2 and 3, a large part of Chap. 4 does not depend on these chapters and can be read independently. In the final chapter on summation and integration (Chap. 5), we sometimes focus on the recurrence case, sometimes on the differential case, and sometimes use the general operator language of Chap. 4.

The book includes hundreds of exercises of varying degrees of difficulty, and we encourage the reader to give them some consideration. The exercises not only allow to check the understanding and train the methods presented in the text, but they sometimes also contain interesting additional ideas. Solutions are provided in the appendix. The number of stars attached to an exercise indicates the length of the solution given in the back and does not necessarily reflect the hardness of the problem. Where I was able to remember the source of inspiration for a particular exercise, e.g., a published paper or an informal discussion, I mention the name of the inspirator(s) in the problem statement or give a citation in the solution.

Throughout the book, I have tried to keep the required background knowledge at a minimum. When there was a choice between an argument that uses some fancy abstract concepts and an argument consisting of an elementary technical calculation, I usually chose the latter. This made some parts of the text more technical than necessary, but I decided to pay this price in order to make the book accessible not only to mathematics students but also to interested students from computer science or physics, for example. Readers without any experience in the manipulation of infinite sequences and formal power series by hand or by computer algebra may wish to study the more elementary book *The Concrete Tetrahedron* by Peter Paule and myself before entering the more advanced treatment in the present book. Conversely, I would like to recommend the present book to readers of *The Concrete Tetrahedron* who would like to know more about the subject.

I have first heard about D-finite functions about 20 years ago when I came to Linz as a Ph.D. student and I have since had the opportunity to discuss their features with a lot of people from all around the world. I would like to take this opportunity to thank Sergei Abramov, Alin Bostan, Manfred Buchacher, Shaoshi Chen, Frédéric Chyzak, Lixin Du, Mark van Hoeij, Hui Huang, Maximilian Jaroschek, Fredrik Johansson, Christoph Koutschan, Ziming Li, Stephen Melczer, Marc Mezzarobba, Marni Mishna, Peter Paule, Marko Petkovšek, Veronika Pillwein, Gleb Pogudin, Clemens Raab, Georg Regensburger, Bruno Salvy, Carsten Schneider, Michael Singer, Thibaut Verron, Rika Yatchak, Doron Zeilberger, Yi Zhang, and Burkhard Zimmermann for many inspiring discussions and exciting collaborations from which I have learned so much. In addition, I would like to thank the anonymous referees, Alin Bostan, Shaoshi Chen, Lixin Du, Gargi Murkherjee, Georg Regensburger, Clemens Raab, and especially Michael Singer and Elaine Wong, for their valuable comments on earlier versions of the manuscript.

Linz, Austria Manuel Kauers
March 2023

Contents

Chapter 1
Background and Fundamental Concepts

1.1 Functions, Sequences, and Series

This book is about doing computations with functions. Given a function, we may for example want to prove certain conjectures about it, to discover new properties of the function, to prove the presence or absence of relations with other given functions, to determine the asymptotic behavior in certain regions, to find a closed form expression for the function, or to prove that no closed form expression exists. A large part of this book deals with algorithms for solving problems of this sort. Before we enter into the subject, we review the fundamental concepts of functions, sequences, and series, and fix some of the notation that we will use in the sequel. Readers unfamiliar with the material will find some references to introductory textbooks at the end of the section. A natural obstruction towards general algorithms for computing with functions will appear, which forces us to restrict to certain classes of functions. After giving an overview of such classes, we proceed to Sect. 1.2, where we introduce the main character of this book: the class of D-finite functions.

Recall the concept of a function. For two sets A, B, a *function* (or *map*) $f: A \to B$ is defined as a subset of $A \times B$ such that for every $a \in A$ there is exactly one $b \in B$ such that (a, b) is an element of the subset. We then say that b is the value of f at a and write $f(a) = b$. By a *sequence* in a set B, we mean a function $f: A \to B$ with $A = \mathbb{N}$ or $A = \mathbb{Z}$. It will be convenient to extend the notion of sequences also to functions defined on a set $A = \alpha + \mathbb{N} = \{\alpha + n : n \in \mathbb{N}\} \subseteq C$ or $A = \alpha + \mathbb{Z} = \{\alpha + n : n \in \mathbb{Z}\} \subseteq C$ for a field C of characteristic zero and fixed $\alpha \in C$. For a sequence $f: A \to B$ with $f(n) = a_n$ for $n \in A$, we use the notations $(a_n)_{n=0}^{\infty}$ (if $A = \mathbb{N}$), $(a_n)_{n\in\mathbb{Z}}$, $(a_n)_{n\in\alpha+\mathbb{N}}$, or $(a_n)_{n\in\alpha+\mathbb{Z}}$, respectively. For example, if F_n is the nth Fibonacci number, then $(F_n)_{n=0}^{\infty}$ is the Fibonacci sequence.

If B is a ring, then the set B^A of all functions $f: A \to B$ together with pointwise addition and multiplication is also a ring. For example, for two sequences $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ in B, their sum $(a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty}$ is the sequence $(a_n + b_n)_{n=0}^{\infty}$ and their product $(a_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty}$ is the sequence $(a_n b_n)_{n=0}^{\infty}$. In the case of sequences, the

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1_1

termwise product is also known as the *Hadamard product,* in order to distinguish it from another type of multiplication, known as the *Cauchy product.* The Cauchy product of two sequences $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ is defined as the sequence $(c_n)_{n=0}^{\infty}$ with $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ for $n \in \mathbb{N}$.

The set of sequences in a ring B also forms a ring with termwise addition and the Cauchy product. To avoid confusion, we will use the notation $B^{\mathbb{N}}$ for the ring of sequences together with termwise addition and the Hadamard product and write $B[[x]]$ for the ring of sequences together with termwise addition and the Cauchy product. Although the elements of $B[[x]]$ are formally not different from those in $B^{\mathbb{N}}$, we call them *formal power series* rather than sequences, and instead of the notation $(a_n)_{n=0}^{\infty}$, we use the notation $\sum_{n=0}^{\infty} a_n x^n$ to denote them. For example, the formal power series x^7 is equal to the sequence $(a_n)_{n=0}^{\infty}$ with $a_7 = 1$ and $a_n = 0$ for all $n \in \mathbb{N} \setminus \{7\}$. We say that a_n is the *coefficient* of x^n in $a := \sum_{n=0}^{\infty} a_n x^n$, and we use the notation $[x^n]a$ to denote the coefficient of x^n in the series a. We also write $a(0)$ instead of $[x^0]a$. Note that as a consequence of the definition of the Cauchy product, we have $x^i x^j = x^{i+j}$ for all $i, j \in \mathbb{N}$. This motivates the notation of formal power series as infinite sums. Note also that the symbol x is not a variable but stands for the particular series $x = x^1 = \sum_{n=0}^{\infty} a_n x^n$ with $a_1 = 1$ and $a_n = 0$ for $n \in \mathbb{N} \setminus \{1\}$. We shall take the freedom to use other expressions in place of x, for example y, $x - 1$, or x^{-1}. Each of the rings $B[[y]]$, $B[[x-1]]$, $B[[x^{-1}]]$ is a copy of the set of all sequences in the ring B endowed with termwise addition and the Cauchy product. Of course, in the case of x^{-1}, we will write x^{-n} instead of $(x^{-1})^n$, analogous to obvious shortcuts such as 1 and x for x^0 and x^1.

The notation for formal power series as infinite sums is also compatible with the point of view that elements of $B[[x]]$ are not sequences $a\colon \mathbb{N} \to B$, which are undefined for negative integers, but that they are sequences $a\colon \mathbb{Z} \to B$ with $a(n) = 0$ for all $n < 0$. If we write these elements in the form $\sum_{n\in\mathbb{Z}} a_n x^n$, we may wonder whether the Cauchy product can be extended to all sequences $(a_n)_{n\in\mathbb{Z}}$ in such a way that $x^i x^j = x^{i+j}$ for all $i, j \in \mathbb{Z}$. It turns out that this is not possible. To see why, consider the product of a series $\sum_{n\in\mathbb{Z}} a_n x^n$ with itself. The coefficient of x^0 in the result will be the sum $\sum_{i+j=0} a_i a_j$, which is not meaningful if there are infinitely many nonzero summands, for example if $a_n = 1$ for all $n \in \mathbb{Z}$. The requirement that $a_n = 0$ for all $n < 0$ ensures that every coefficient in the product of two series is a sum with only finitely many nonzero summands. This requirement is sufficient, but not necessary. We can more generally allow all sequences $(a_n)_{n\in\mathbb{Z}}$ for which there exists some $n_0 \in \mathbb{Z}$ such that $a_n = 0$ for all $n < n_0$. The set of all these sequences together with termwise addition and the natural extension of the Cauchy product is denoted by $B((x))$ and called the ring of *formal Laurent series.* For each formal Laurent series $f = \sum_{n\in\mathbb{Z}} a_n x^n$, except for the zero series, there is a smallest index $n \in \mathbb{Z}$ such that $a_n \neq 0$. This n is called the *order* or the *valuation* of the series and is denoted by $\operatorname{ord}(f)$ or $\nu(f)$. The order of the zero sequence is defined as $+\infty$. Again, we take the freedom to use different expressions such as y, $x - 1$, or x^{-1} in place of x. Note that when we write an element of $B((x^{-1}))$ in the form $\sum_{n\in\mathbb{Z}} a_n x^n$, then its order is the *largest* index n with $a_n \neq 0$.

Besides enlarging the index range of the coefficients of a series, we can also shrink it. For example, we may consider all series $\sum_{n=0}^{\infty} a_n x^n$ for which there exists a $d \in \mathbb{N}$ such that $a_n = 0$ for all $n > d$. Such series are called *polynomials*. The set of all polynomials is denoted by $B[x]$. It is a subring of $B[[x]]$. The largest number $d \in \mathbb{N}$ with $a_d \neq 0$ is called the *degree* of the polynomial, and is denoted by $\deg(p)$ or $\deg_x(p)$. Such a d exists unless $a_n = 0$ for all $n \in \mathbb{Z}$. This is only the case for the zero polynomial, whose degree we define as $-\infty$. Alternatively, we may consider all series $\sum_{n\in\mathbb{Z}} a_n x^n$ for which there exists a $d \in \mathbb{N}$ such that $a_n = 0$ for all $n \in \mathbb{Z}$ with $|n| > d$. Such series are called *Laurent polynomials*. The set of all Laurent polynomials is denoted by $B[x, x^{-1}]$. It is a subring of $B((x))$. It can also be viewed as a subring of $B((x^{-1}))$.

In the following theorem, we collect some properties about the multiplication of series. Recall that a ring B is called an *integral domain* if for any $u, v \in B \setminus \{0\}$ we have that $uv \neq 0$.

Theorem 1.1 *Let B be a commutative ring.*

1. *If B is an integral domain, then so are $B[x]$, $B[[x]]$, and $B((x))$.*
2. *$f \in B[[x]]$ has a multiplicative inverse in $B[[x]]$ if and only if the coefficient $f(0) = [x^0]f \in B$ has a multiplicative inverse in B.*
3. *$f \in B((x))$ has a multiplicative inverse in $B((x))$ if and only if $f \neq 0$ and the coefficient $[x^{\nu(f)}]f \in B$ has a multiplicative inverse in B.* □

Proof

1. Since $B[x] \subseteq B[[x]] \subseteq B((x))$, it suffices to show the claim for $B((x))$. Let $u, v \in B((x)) \setminus \{0\}$. Their orders $\nu(u), \nu(v)$ are finite. By the definition of order, $[x^{\nu(u)}]u$ and $[x^{\nu(v)}]v$ are nonzero. We have $[x^{\nu(u)+\nu(v)}](uv) = \sum_{i+j=\nu(u)+\nu(v)}([x^i]u)([x^j]v)$, where the sum runs over all pairs $(i, j) \in \mathbb{Z}^2$ with $i + j = \nu(u) + \nu(v)$. If $i < \nu(u)$, then $[x^i]u = 0$ by the definition of $\nu(u)$, and if $i > \nu(u)$, then $j < \nu(v)$, so $[x^j]v = 0$ by the definition of $\nu(v)$. Hence, all terms in the sum are zero, except possibly $([x^{\nu(u)}]u)([x^{\nu(v)}]v)$. Since B is an integral domain and $[x^{\nu(u)}]u$, $[x^{\nu(v)}]v$ are both nonzero, this term is also nonzero, so uv has a nonzero coefficient and is therefore not the zero series.
2. "$\Rightarrow$": If $g \in B[[x]]$ is a multiplicative inverse of $f \in B[[x]]$, then $fg = 1$, which implies $[x^0](fg) = [x^0]1 = 1$. By the definition of the Cauchy product we have $[x^0](fg) = ([x^0]f)([x^0]g)$ for all $f, g \in B[[x]]$. Therefore $[x^0]g$ is a multiplicative inverse of $[x^0]f$.
   "$\Leftarrow$": Let $f \in B[[x]]$ be such that $[x^0]f$ has a multiplicative inverse $b \in B$, i.e., $b[x^0]f = 1$. We have to show that there exists a series $g = \sum_{n=0}^{\infty} a_n x^n$ such that $gf = 1$. Extracting the coefficient of x^n on both sides gives the requirement $\sum_{k=0}^{n} a_k[x^{n-k}]f = [x^n]1$ for the coefficient sequence of g. After multiplying by b, we obtain the recurrence $a_n = b[x^n]1 - \sum_{k=0}^{n-1} a_k b[x^{n-k}]f$ $(n \in \mathbb{N})$. Since for every $n \in \mathbb{N}$, the right hand side involves only the terms $a_0, \ldots, a_{n-1}$ (besides the known coefficients of f), it can be shown by induction on n that

this recurrence equation has a unique solution. (Its first terms are $a_0 = b$, $a_1 = -b^2[x^1]f$, $a_2 = b^3([x^1]f)^2 - b^2[x^2]f$.) This completes the proof.
3. Since $f = x^{\nu(f)}g$ for some $g \in B[[x]]$ with $[x^0]g = [x^{\nu(f)}]f$, and since $f^{-1} = x^{-\nu(f)}g^{-1}$ provided that the inverses exist, the claim follows directly from part 2. ∎

Example 1.2

1. For any fixed $\alpha \in B$, The series $1 - \alpha x \in B[[x]]$ has the multiplicative inverse $\sum_{n=0}^{\infty} \alpha^n x^n$, the so-called *geometric series.* Indeed, $(1 - \alpha x)\sum_{n=0}^{\infty} \alpha^n x^n = \sum_{n=0}^{\infty} \alpha^n x^n - \sum_{n=1}^{\infty} \alpha^n x^n = 1$.
2. The series $\exp(x) := \sum_{n=0}^{\infty} \frac{1}{n!}x^n \in \mathbb{Q}[[x]]$ has the multiplicative inverse $\sum_{n=0}^{\infty} \frac{(-1)^n}{n!}x^n \in \mathbb{Q}[[x]]$. Indeed,

$$\Big(\sum_{n=0}^{\infty} \frac{1}{n!}x^n\Big)\Big(\sum_{n=0}^{\infty} \frac{(-1)^n}{n!}x^n\Big) = \sum_{n=0}^{\infty}\Big(\sum_{k=0}^{n} \frac{1}{k!}\frac{(-1)^{n-k}}{(n-k)!}\Big)x^n$$
$$= \sum_{n=0}^{\infty}\Big(\sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\Big)\frac{1}{n!}x^n = \sum_{n=0}^{\infty}(1-1)^n\frac{1}{n!}x^n = 1.$$

In this derivation, we used the binomial theorem $\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = (a+b)^n$. See Exercise 4 for a more general form. Also observe that the convention $0^0 = 1$ enters.
3. Let $p_0 = 1$ and $p_n \in \mathbb{N}$ be the nth prime number for $n \in \mathbb{N}$. The series $a(x) = \sum_{n=0}^{\infty} p_n x^n \in \mathbb{Z}[[x]]$ has a multiplicative inverse. There seems to be no simple general expression for the nth coefficient of the series $1/a(x)$. However, the proof of part 2 of the theorem allows us to compute as many coefficients of $1/a(x)$ as we desire. The first few terms turn out to be

$$\frac{1}{a(x)} = 1 - 2x + x^2 - x^3 + 2x^4 - 3x^5 + 7x^6 - 10x^7 + 13x^8 - 21x^9 + 26x^{10} + \cdots$$

□

Theorem 1.1 implies that for a field C, the set $C[[x]]$ is an integral domain and $C((x))$ is a field. The field $C((x))$ is (isomorphic to) the quotient field of $C[[x]]$. The quotient field of $C[x]$, denoted by $C(x)$, is called the field of *rational functions.* Its elements are simply fractions of polynomials, on which the arithmetic operations are defined in the obvious way. We can identify the field $C(x)$ with a certain subfield of $C((x))$. For example, the rational function $\frac{1}{1-x}$ corresponds to the geometric series $1 + x + x^2 + x^3 + \cdots$, because this is the multiplicative inverse of $1 - x$ in $C((x))$. Alternatively, the field $C(x)$ can also be identified with a certain subfield of $C((x^{-1}))$. In this case, the element $\frac{1}{1-x}$ of $C(x)$ corresponds to the series $-x^{-1} - x^{-2} - x^{-3} - \cdots$, which is the multiplicative inverse of $1 - x$ when interpreted as an element of $C((x^{-1}))$. When we view $C(x)$ as a subfield of $C((x-1))$, the series corresponding to $\frac{1}{1-x}$ is particularly simple: it just consists of the single term $-(x-1)^{-1}$.

The argument given in the proof of part 2 of Theorem 1.1 is typical for justifying that certain series exist. It boils down to the observation that each particular coefficient of the desired series can be computed using a finite number of operations. Also the definition of the Cauchy product is only meaningful because the nth coefficient of the product is specified by a sum of $n+1$ terms. The same idea can be used to define further operations. For example, if we have a sequence of series, i.e., $(f_n)_{n=0}^{\infty}$ with $f_n \in C[[x]]$ for each n, the sum $\sum_{n=0}^{\infty} f_n$ of all of these series is usually not well-defined, because its coefficients $[x^k]\sum_{n=0}^{\infty} f_n = \sum_{n=0}^{\infty}[x^k]f_n$ may be infinite sums. But if we have an additional property that guarantees that these sums are finite, then we are fine. For example, if we have $\nu(f_n) \geq n$ for all $n \in \mathbb{N}$, then $[x^k]\sum_{n=0}^{\infty} f_n = \sum_{n=0}^{\infty}[x^k]f_n = \sum_{n=0}^{k}[x^k]f_n$, because $[x^k]f_n = 0$ for all $n > k$. One application of this observation is that the standard notation that we use for expressing formal power series, $\sum_{n=0}^{\infty} a_n x^n$, can be viewed as the infinite sum over all series $f_n = a_n x^n$ consisting of (at most) one term. Note that $\nu(a_n x^n) \geq n$. Another application is the composition of formal power series. For $f = \sum_{n=0}^{\infty} a_n x^n \in B[[x]]$ and $g \in B[[x]]$ with $\nu(g) \geq 1$ we define $f(g)$ as the infinite sum $\sum_{n=0}^{\infty} a_n g^n$, and this sum is a well-defined formal power series because we have $\nu(g^n) = n\nu(g) \geq n$ for all $n \in \mathbb{N}$. Of course, no restriction is needed for the composition of polynomials: for any $p = \sum_{i=0}^{d} p_i x^i$ and $q \in B[x]$, the composition $p(q) = \sum_{i=0}^{d} p_i q^i \in B[x]$ is well-defined.

The implicit function theorem is another feature of formal power series, and its justification also rests on the observation that each coefficient of a series can be computed by finitely many operations. More precisely, given a formal power series $f \in B[[x,y]] := B[[x]][[y]]$, the question is whether the equation $g(x) = f(x, g(x))$ has a solution $g \in B[[x]]$. The answer is that such a solution exists (at least) if $[x^0][y^0]f = [x^0][y^1]f = 0$. To see why a solution exists in this case, write $f = \sum_{n=0}^{\infty}\big(\sum_{k=0}^{\infty} a_{n,k}x^k\big)y^n$ with $a_{0,0} = a_{0,1} = 0$ and make an ansatz $g(x) = \sum_{\ell=0}^{\infty} b_\ell x^\ell$ with undetermined coefficients b_ℓ. The equation $g(x) = f(x, g(x))$ is satisfied if and only if $b_\ell = [x^\ell]f(x, g(x))$ for all $\ell \in \mathbb{N}$. Because of $a_{0,0} = 0$, the choice $b_0 = 0$ will meet this requirement for $\ell = 0$. With this choice, we will have $\nu(g) \geq 1$ and $\nu(g^n) \geq n$ for all $n \in \mathbb{N}$. Therefore, for $\ell > 0$, we have

$$[x^\ell]f(x, g(x)) = [x^\ell]\sum_{n=0}^{\infty}\Bigg(\sum_{k=0}^{\infty} a_{n,k}x^k\Bigg)g^n = [x^\ell]\sum_{n=0}^{\ell}\Bigg(\sum_{k=0}^{\ell} a_{n,k}x^k\Bigg)g^n$$
$$= \sum_{n=0}^{\ell}\sum_{k=0}^{\ell} a_{n,k}[x^\ell]x^k g^n = \sum_{n=0}^{\ell}\sum_{k=0}^{\ell} a_{n,k}[x^{\ell-k}]g^n.$$

By the assumption $a_{0,0} = a_{0,1} = 0$, we only need to care about n, k with $n \geq 1$ or $k > 1$, and in these cases, the coefficient $[x^{\ell-k}]g^n$ only depends on $b_0, \ldots, b_{\ell-1}$. Therefore, the requirements $b_\ell = [x^\ell]f(x, g(x))$ and $b_0 = 0$ amount to a recurrence for the coefficient sequence $(b_\ell)_{\ell=0}^\infty$ of the solution g, and this recurrence has a unique solution.

Example 1.3

1. For a given $f \in C[[x]]$ with $[x^0]f = 0$ and $[x^1]f \neq 0$, the implicit function theorem implies the existence of a *compositional inverse,* i.e., a series $g \in C[[x]]$ with $[x^0]g = 0$ such that $f(g(x)) = x$. For example, the series $f = \exp(x)-1 = x + \frac{1}{2}x^2 + \frac{1}{6}x^2 + \cdots$ has a functional inverse. We can compute its terms by following the argument outlined above. The first terms turn out to be
$$x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 + \tfrac{1}{5}x^5 - \tfrac{1}{6}x^6 + \cdots.$$
The implicit function theorem does not give us directly that the nth term of the inverse is $\frac{(-1)^n}{n}x^n$, but we will see shortly that this is the case.
2. By the implicit function theorem, an equation $h(x, g(x)) = 0$ has a solution $g(x) \in B[[x]]$ if $[x^0][y^0]h = 0$ and $[x^0][y^1]h$ has a multiplicative inverse in B, because in this case we can rewrite the equation in the form $g(x) = f(x, g(x))$ for a series $f \in B[[x, y]]$ with $[x^0][y^0]f = [x^0][y^1]f = 0$. For example, for the series
$$h(x, y) = (x-4)x+(5x^2+3x+3)y+(2x^2-5)y^2+(x-1)(2x-3)y^3 \in \mathbb{Q}[[x, y]]$$
the equation $h(x, g(x)) = 0$ has a solution $g(x) \in \mathbb{Q}[[x]]$. Its first terms can be computed by following the argument outlined above. It turns out that
$$g(x) = \tfrac{4}{3}x + \tfrac{35}{27}x^2 - \tfrac{31}{243}x^3 - \tfrac{8633}{2187}x^4 - \tfrac{242860}{19683}x^5 - \tfrac{1664381}{59049}x^6 - \tfrac{27257935}{531441}x^7 + \cdots.$$

□

Formal power series are called "formal" in order to distinguish them from the concept of power series known from calculus. One difference is that the coefficients of formal power series need not be real or complex numbers, but can belong to an arbitrary ring B. A second difference is that the symbol x used in the notation of formal power series is not a "variable" which we could replace by some element of B. In fact, such a substitution would almost always lead to a meaningless infinite sum. Instead, a formal power series is nothing more than the sequence of its coefficients, and x stands for the particular series with $[x^1]x = 1$ and $[x^n]x = 0$ for $n \neq 1$. In the following, when we say "power series" or simply "series", we mean formal power series (or, perhaps, formal Laurent series), unless we explicitly say that we mean power series in the sense of calculus. Our convention is to restrict the use of x to algebraic objects and use other names to denote evaluation points. For example, we might say that $p(z)$ is the value of the polynomial $p = p(x) \in B[x]$ at the evaluation point $z \in B$. Other identifiers $(y, z, n, k, \ldots)$ will sometimes be used as variables and sometimes as algebraic objects, which hopefully does not cause too much confusion. For example, the symbol n will often denote some integer, but in the polynomial ring $C[n]$, it plays exactly the same role as x.

Despite the algebraic nature of formal power series, we do have a notion of differentiating them. For a series $a(x) = \sum_{n=0}^{\infty} a_n x^n \in B[[x]]$, the *derivative* $a'(x)$ is defined as $a'(x) := \sum_{n=0}^{\infty} a_{n+1}(n+1)x^n$. It is clear that the sum of the derivatives of two series is the derivative of the sum of these series. Moreover, the product rule and the chain rule known from calculus carry over to the formal power series setting (Exercise 12). As a first application of differentiation for formal power series, let us prove that the series $\log(1+x) \in \mathbb{Q}[[x]]$ defined as $\log(1+x) := \sum_{n=0}^{\infty} \frac{(-1)^n}{n+1} x^{n+1}$ is indeed the compositional inverse of the series $\exp(x) - 1 \in \mathbb{Q}[[x]]$ with $\exp(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$. By the definition of differentiation, we have $\log'(1+x) = \sum_{n=0}^{\infty} (-1)^n x^n$, which by Example 1.2 is the multiplicative inverse of the series $1 + x \in \mathbb{Q}[[x]]$. We thus have $\log'(1+x) = \frac{1}{x+1}$, like in calculus. Even more easily, it follows from the definition of differentiation that $\exp'(x) = \exp(x)$, also as expected. Therefore, by the chain rule, the derivative of the composition $\exp(\log(1+x))$ is $\exp(\log(1+x))\frac{1}{1+x}$, and by the chain and product rules, the derivative of this series is

$$\exp(\log(1+x))\Big(\frac{1}{1+x}\Big)^2 + \exp(\log(1+x))\frac{-1}{(1+x)^2} = 0.$$

It follows that $[x^n]\exp(\log(1+x)) = 0$ for all $n \geq 2$. It remains to figure out the coefficients of x^0 and x^1, which can be easily done using the formula by which the composition was defined. It turns out that we have the identity $\exp(\log(1+x)) = 1 + x$ in $\mathbb{Q}[[x]]$.

Having the operation of differentiation in our portfolio allows us to speak about differential equations, and to ask for the series they have as solutions. In order to prove the existence of a power series solution, it is often possible to apply similar arguments as above for justifying the existence of multiplicative inverses, the composition, or solutions to functional equations.

Example 1.4 We want to show that the differential equation $f'(x) = \exp(f(x))/(1 + f(x))$ has a unique solution $f \in \mathbb{Q}[[x]]$ with $f(0) = 0$. Consider a formal power series $f(x) = \sum_{n=1}^{\infty} a_n x^n$. In order for this series to be a solution of the differential equation, we must have $[x^n]f'(x) = [x^n]\exp(f(x))/(1 + f(x))$ for all $n \in \mathbb{N}$. On the left we have $(n+1)a_{n+1}$ while the right hand side is a certain mess which only depends on $a_1, \ldots, a_n$. The relation therefore allows us to compute all of the coefficients of a solution series $f(x)$ for the equation, one at a time. The result turns out to be

$$f(x) = x + \tfrac{1}{6}x^3 - \tfrac{1}{12}x^4 + \tfrac{13}{120}x^5 - \tfrac{37}{360}x^6 + \tfrac{593}{5040}x^7 - \tfrac{883}{6720}x^8 + \tfrac{55781}{362880}x^9 + \cdots.$$

□

Much of the material in this text applies to any setting where there is an addition, a multiplication, and a differentiation. The ring of formal power series is an example for such a setting. Another example is the set of analytic functions, say from $\mathbb{C}$ to $\mathbb{C}$. This set forms a ring together with pointwise addition and multiplication, and there is a natural notion of differentiation. More generally, we may consider meromorphic functions defined on a certain open subset of $\mathbb{C}$, or on a certain Riemann surface. It is also possible to consider the set of all smooth functions defined on a certain subset A of the reals.

Our goal is to develop algorithms for doing computations with functions. Informally speaking, an *algorithm* is a procedure which takes some input, performs certain operations, and returns some output after a finite amount of time. It adheres to a *specification* which declares how the input and the output of the algorithm are related to one another. The algorithm is *correct* if it meets the announced specification. The official formal definition of what an algorithm is involves a number of technical details that are not really relevant for our purpose, and we will not discuss them here. We must emphasize however that every algorithm can only process a finite amount of information at a time. In particular, the input and the output of an algorithm must always be "finite": in order to do computations with mathematical objects, we need to encode them in some way as finite strings of characters from a certain fixed alphabet, e.g., $\{0, 1\}$. For example, an integer can be encoded by a sign followed by the list of its digits in some fixed base, e.g., 2. In order to encode a rational number, we can encode its numerator, followed by a separator symbol such as "/", followed by an encoding of its denominator.

Rings and fields are called *computable* if there is a way to encode their elements as finite strings and there are algorithms for performing the arithmetic operations and for checking whether two given encodings represent the same element. The bad news is that formal power series rings are not computable. The reason is that from a finite number of characters, we can only form countably many finite strings, while the number of sequences $f: \mathbb{N} \to \{0, 1\}$, and thus the number of formal power series with coefficients in some ring, is uncountable. For the same reason, there is no way to encode analytic or meromorphic functions, and in fact no way to encode real or complex numbers. There are just too many of them. If we want to do computations with formal power series or real or complex functions nevertheless, we are forced to make some concessions. One option is to resort to *approximation.* For example, instead of insisting that the input of an algorithm be any specific real number z, which is not possible, we may have an algorithm that takes as input a rational number ζ and a positive integer N so that $|z - \zeta| < 2^{-N}$, and whose output allows us to make some statement about any real number whose distance to ζ is less than 2^{-N}. Similarly, instead of insisting that the input of an algorithm be any continuous function $f: [0, 1] \to \mathbb{R}$, which is not possible, we may have an algorithm that takes as input a finite list $(y_0, y_1, \ldots, y_n)$ where each y_k $(k = 0, \ldots, n)$ is an approximation of the value $f(k/n)$ of f at k/n. The algorithm may deliver some output that allows us to draw some conclusions about f. Finally, instead of insisting that the input of an algorithm be any formal power series $f \in B[[x]]$, which is not possible, we may have an algorithm that takes as input the first n terms of a power series and produces some output which is valid for all power series that start with the terms supplied as input. Some of the arguments we used earlier to define operations on power series give rise to algorithms of this kind.

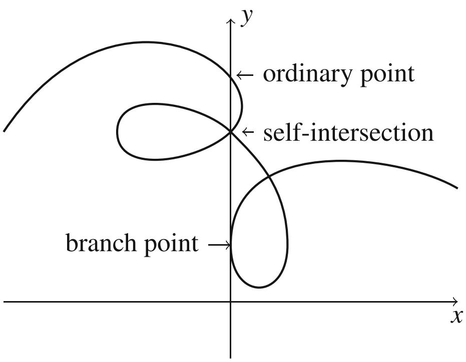
Approximation is a truly powerful computational paradigm, but it is not useful in every context. There is another powerful computational paradigm for resolving the issue that the domain of interest is too large to admit an encoding that is suitable for doing computations. The idea is to restrict the attention to a smaller domain. While we cannot compute in $\mathbb{R}$, nothing prevents us from doing computations in the smaller field $\mathbb{Q}$. Similarly, we can identify classes of formal power series or analytic functions that are sufficiently restricted so that computations in them are possible. This can be done in many ways. In the following examples, and in fact throughout the rest of this book, C is an arbitrary field of characteristic zero (i.e., a field in which all of the elements $\sum_{k=1}^{n} 1$ for $n \geq 1$ are nonzero). When C appears in statements related to computation, it is further assumed that C is computable.

Example 1.5

1. If C is computable, then so is the polynomial ring $C[x]$, i.e., the subring of $C[[x]]$ consisting of series with only finitely many nonzero coefficients. There are plenty of problems which can be solved algorithmically in $C[x]$. The corresponding algorithms form the heart of computer algebra. Some of the main results are summarized in Sect. 1.4.
   Rational series form a larger subclass of $C[[x]]$. A series $f \in C[[x]]$ is called *rational* if we have $f = p/q$ for some $p, q \in C[x] \subseteq C[[x]]$. It can be checked (Exercise 15) that a series $\sum_{n=0}^{\infty} a_n x^n$ is rational if and only if the sequence $(a_n)_{n=0}^{\infty}$ satisfies a linear recurrence equation with constant coefficients, i.e., if there are $c_0, \dots, c_r \in C$, not all zero, such that
   $$c_0 a_n + c_1 a_{n+1} + \cdots + c_r a_{n+r} = 0$$
   for all $n \in \mathbb{N}$. Such sequences are also called *C-finite*. For example, the Fibonacci sequence is C-finite, and we have $\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}$.
   The class of rational series forms a computable subring of $C[[x]]$.
2. Polynomials and rational series are very small classes. At the other extreme, a very big class consists of the so-called computable series. A series $\sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ is called *computable* if there exists an algorithm which for any given $n \in \mathbb{N}$ computes the nth coefficient a_n of the series. In this case, we also say that $(a_n)_{n=0}^{\infty}$ is a computable sequence. Examples for computable sequences include the sequence of prime numbers, the decimal digits of constants like π or $\sqrt{2}$, or the sequence whose nth term is the number of unlabeled trees with n nodes.
   A computable series or sequence can be encoded by writing down an algorithm that computes its terms. Note that this is a finite representation.
   Computable series form a ring, because when we are given algorithms for computing the nth term of some series a, b, then we can construct from them an algorithm that computes the nth term of their sum $a + b$ or their

product ab, so these series are computable too. Also the multiplicative inverse, the composition, and the compositional inverse of computable series are easily seen to be computable (provided they exist).
The ring of computable series is not a computable ring, because there is no algorithm which for two computable sequences, each specified by an algorithm, decides whether they are actually equal. This is a consequence of Rice's theorem in theoretical computer science.

3. A series $g \in C[[x]]$ is called *algebraic* if there is a nonzero polynomial $p \in C[x, y] := C[x][y]$ such that $p(x, g(x)) = 0$.
If C is an algebraically closed field, any univariate polynomial of degree d has d roots in C. Using the implicit function theorem, it can be shown that for each simple root η of $p(0, y) \in C[y]$, there is exactly one series $g(x)$ with $g(0) = \eta$ and $p(x, g(x)) = 0$. In this case, the algebraic series is uniquely determined by p and η, and we can use this data as an encoding.
If η is a multiple root of $p(0, y)$, there may be several series $g(x)$ with $g(0) = \eta$ and $p(x, g(x)) = 0$, or none, depending on the geometry of the curve consisting of all points $(\zeta, \eta) \in C^2$ with $p(\zeta, \eta) = 0$. Each "branch" of the curve passing through the point $(0, \eta)$ gives rise to a separate solution $g(x)$ with $g(0) = \eta$. Some of these may not only share the same coefficient of x^0, but also agree on some finitely many more initial terms. In any event, a particular solution is uniquely determined by the polynomial p and a finite number of initial coefficients.
Branches for which the tangent at the point $(0, \eta)$ is vertical do not give rise to formal power series solutions. However, it can be shown that if η is a root of $p(0, y)$ of multiplicity m, there is an $r \in \{1, \ldots, m\}$ such that there are m distinct formal power series $g(x) \in C[[x]]$ with $g(0) = \eta$ and $p(x^r, g(x)) = 0$. The smallest such r is called the *ramification index* of the point $(0, \eta)$, and this point is called a *branch point* if $r > 1$. If $g(x)$ is such that $p(x^r, g(x)) = 0$, then we can say that $p(x, g(x^{1/r})) = 0$, where $g(x^{1/r}) \in C[[x^{1/r}]]$ is a formal power series whose exponents are integer multiples of $1/r$.



There is also the possibility that the degree of $p(0, y)$ in y is smaller than the degree $p(x, y)$ in y. In this case, there are some series solutions involving negative exponents.

For algebraically closed fields C, a nontrivial but fundamental result in the theory of algebraic functions asserts that for every irreducible polynomial $p \in C[x, y]$ there exists a positive integer r and $\deg_y p$ many distinct Laurent series $g \in C((x))$ such that $p(x^r, g(x)) = 0$. If $g \in C((x))$ is any formal Laurent series, and r is a positive integer, the series $g(x^{1/r}) \in C((x^{1/r}))$ is called a *Puiseux series*. More generally, the result says that the set of all Puiseux series over an algebraically closed field C is itself an algebraically closed field.

Another nontrivial but fundamental result is that the set of algebraic series is a computable subring of $C[[x]]$ and that this ring is closed under differentiation.

4. Some series can be encoded by explicit expressions for their coefficient sequences. An example is the class of *hypergeometric series*. A series $\sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ is called *hypergeometric* if there are constants $\alpha_1, \ldots, \alpha_p$, $\beta_1, \ldots, \beta_q \in C$ such that

$$a_n = \frac{\alpha_1^{\overline{n}} \cdots \alpha_p^{\overline{n}}}{\beta_1^{\overline{n}} \ldots \beta_q^{\overline{n}} n!}$$

for all $n \in \mathbb{N}$. Here $u^{\overline{n}} := u(u+1)\cdots(u+n-1)$ denotes the nth *rising factorial.* Note that $u^{\overline{n}}$ vanishes for $u \in \{0, -1, -2, \ldots, -n+1\}$. Therefore, for a_n to be well-defined, the constants $\beta_1, \ldots, \beta_q$ should not be negative integers, nor zero. The traditional notation for hypergeometric series is

$${}_pF_q\left(\begin{matrix}\alpha_1, \ldots, \alpha_p \\ \beta_1, \ldots, \beta_q\end{matrix} \,\middle|\, x\right) := \sum_{n=0}^{\infty} \frac{\alpha_1^{\overline{n}} \cdots \alpha_p^{\overline{n}}}{\beta_1^{\overline{n}} \ldots \beta_q^{\overline{n}} n!} x^n.$$

For example, we have

$$\begin{aligned}
&{}_0F_0\left(\begin{matrix}- \\ -\end{matrix} \,\middle|\, x\right) = \exp(x), && {}_1F_0\left(\begin{matrix}\alpha \\ -\end{matrix} \,\middle|\, x\right) = (1+x)^{\alpha}, \\
&{}_0F_1\left(\begin{matrix}- \\ 1/2\end{matrix} \,\middle|\, -\frac{x^2}{4}\right) = \cos(x), && {}_0F_1\left(\begin{matrix}- \\ 3/2\end{matrix} \,\middle|\, -\frac{x^2}{4}\right) = x^{-1}\sin(x), \\
&{}_2F_1\left(\begin{matrix}1, 1 \\ 2\end{matrix} \,\middle|\, x\right) = -x^{-1}\log(1-x), && {}_2F_1\left(\begin{matrix}1/2, 1 \\ 3/2\end{matrix} \,\middle|\, -x^2\right) = x^{-1}\arctan(x).
\end{aligned}$$

Many more relevant functions can be expressed in terms of hypergeometric series. The $p+q$ parameters $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$ can be used for encoding a hypergeometric series.

Typically, a series of interest is not itself hypergeometric. More common are series which can be written as linear combinations of some series of the form $a(x)\,{}_pF_q\left(\begin{matrix}\alpha_1,\dots,\alpha_p\\ \beta_1,\dots,\beta_q\end{matrix}\,\middle|\, b(x)\right)$, where $a(x)$ and $b(x)$ are certain algebraic series.

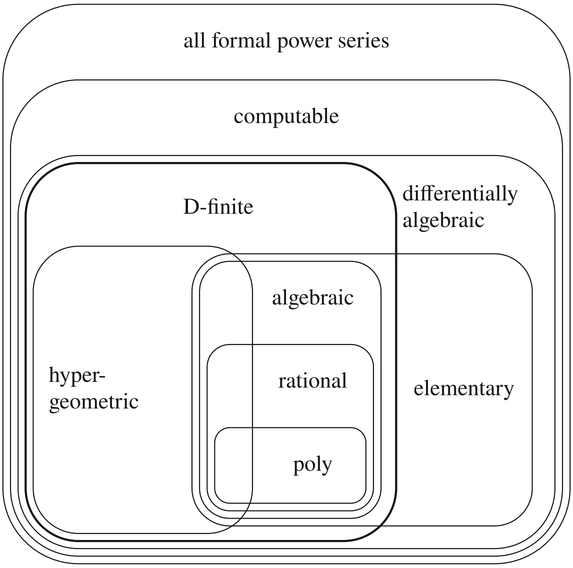
5. Expressions which are formed from constants (i.e., elements from a prescribed field C) and a variable x using the field operations and the operations exp and log, as well as algebraic functions, are called *elementary*. For example,

$$\frac{1 - x^2 + 9x^3 - \exp\left(\frac{1-\sqrt{1+x\exp(-x)}}{1+\sqrt{1-x}}\right)}{1 + x^2 - 3\log\left(1+\sqrt{1+3x+\exp(x^2)}\right)}$$

is an elementary expression.
A formal power series is called elementary if it can be described by an elementary expression. Real and complex functions which can be defined via elementary expressions are called elementary functions. Note that if C includes $\mathrm{i} = \sqrt{-1}$, then sine and cosine are elementary, because we can define them through $\sin(x) = \frac{1}{2\mathrm{i}}(\exp(\mathrm{i}x) - \exp(-\mathrm{i}x))$ and $\cos(x) = \frac{1}{2}(\exp(\mathrm{i}x) + \exp(-\mathrm{i}x))$, respectively.
Elementary power series form a computable subring of $C[[x]]$.

6. A formal power series $f \in C[[x]]$ is called *differentially algebraic* if there is a nonzero polynomial $p \in C[y_0,\dots,y_n]$ such that $p(f, f',\dots,f^{(n)}) = 0$. Here $f^{(i)}$ denotes the ith derivative of f. It turns out that f is uniquely determined by p and a certain finite number of initial terms. The set of differentially algebraic series is a computable subring of $C[[x]]$. □

The choice of a class is influenced by two conflicting design goals. On the one hand, it is desirable that a class is large, so as to maximize the chances that series arising in applications are contained in the class. On the other hand, it is desirable to have a small class, so as to maximize the chances that relevant questions about its elements can be answered by means of efficient algorithms. The class of D-finite series, to which we turn in the next section, has proved to be a good compromise between these two goals. It contains the class of hypergeometric series and the class of algebraic series, has a nontrivial overlap with the class of elementary series, and is itself properly contained in the class of differentially algebraic series. The mutual inclusions are illustrated in the following diagram.



Exercises

1⋆. Is it fair to say that $B[x, x^{-1}]$ is the intersection of $B((x))$ and $B((x^{-1}))$?

2⋆⋆⋆. Show that the Cauchy product is associative.

3. What is the difference between $C[x][[y]]$ and $C[[y]][x]$?

4⋆⋆. For $\alpha \in C$ and $n \in \mathbb{N}$, the *binomial coefficient* $\binom{\alpha}{n}$ is defined as $\frac{\alpha^{\underline{n}}}{n!}$, where $\alpha^{\underline{n}} := \alpha(\alpha-1)\cdots(\alpha-n+1)$ denotes the *falling factorial*. The expression $(1+x)^\alpha$ is defined as the formal power series $\sum_{n=0}^{\infty}\binom{\alpha}{n}x^n$.

a. Show that $(1+x)^\alpha(1+x)^\beta = (1+x)^{\alpha+\beta}$ for all $\alpha, \beta \in C$.
b. Show that $((1+x)^\alpha)' = \alpha(1+x)^{\alpha-1}$ for all $\alpha \in C$.
c. Show that $((1+x)^\alpha)^\beta = (1+x)^{\alpha\beta}$ for all $\alpha, \beta \in C$. By the series on the left, we mean the composition of $(1+x)^\alpha - 1$ into the series $(1+x)^\beta$.

Hint: For part c., use parts a. and b. and the derivation rules of Exercise 12 to show that the derivative of the quotient is 0.

5. Show that the meaning of $(1+x)^\alpha \in C[[x]]$ as introduced in the previous exercise is consistent with the common meaning of $(1+x)^\alpha$ as **a.** a polynomial if $\alpha \in \mathbb{N}$; **b.** a rational series if $\alpha \in \mathbb{Z}$; **c.** an algebraic series if $\alpha \in \mathbb{Q}$.

6⋆. If B is a noncommutative ring, then $B[[x]]$ as defined in the text is a noncommutative ring in which x commutes with every element of B. Generalize Theorem 1.1 to this setting: Show that a series $\sum_{n=0}^{\infty} a_n x^n$ has a two-sided multiplicative inverse in $B[[x]]$ whenever a_0 has a two-sided multiplicative inverse in B.

7. What are the first few terms of the series in $C((x-1))$ and $C((x+1))$ that correspond to the rational function $\frac{x}{1-x-x^2}$?

Hint: Throughout this text, the reader is encouraged to use computer algebra whenever appropriate.

8. Explain why the infinite product $\prod_{n=1}^{\infty}(1-x^n)$ is a well-defined element of $\mathbb{Z}[[x]]$.

9. Let $f \in C[[x^{-1}]]$ and $g \in C((x))$ with $\nu(g) < 0$. Show that the composition $f(g(x))$ is well-defined.

10. Show that the equation $x^2-xy+x^2y-xy^2+y^3=0$ has a unique solution $f \in \mathbb{Q}[[x]]$ with $f(0)=0$, even though the implicit function theorem is not applicable.

11⋆. In Example 1.3 we discussed the inner inverse of a power series $f \in C[[x]]$. This is a series $g \in C[[x]]$ with $f(g(x)) = x$. Show that under the same assumptions on f, there also exists an outer inverse, i.e., a series $h \in C[[x]]$ with $h(f(x)) = x$. How are the outer and the inner inverse related?

12. Show that the product rule $(uv)' = u'v + uv'$ and the chain rule $(u \circ v)' = (u' \circ v)v'$ hold for formal power series $u, v \in B[[x]]$.

13. Compute the first few terms of the formal power series $f \in \mathbb{Q}[[x]]$ with $f(0) = 0$ and $f'(x) = \cos(f(x))$, where $\cos(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n} \in \mathbb{Q}[[x]]$.

14. A real number $z \in \mathbb{R}$ is called computable if there is an algorithm that computes for any given $n \in \mathbb{N}$ the nth digit in the decimal expansion of z. Prove or disprove: If the number $z \in \mathbb{R}$ is not computable, then the field $\mathbb{Q}(z) \subseteq \mathbb{R}$ is not computable either.

15⋆. Show that a sequence $(a_n)_{n=0}^{\infty}$ in C is C-finite if and only if the series $\sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ is rational.

16⋆. Let a_n be the nth digit in the decimal expansion of $\sqrt{2}$ ($a_0 = 1$, $a_1 = 4$, $a_2 = 1, \ldots$). Show that the sequence $(a_n)_{n=0}^{\infty}$ is not C-finite.

17. Let $a \in C[[x]]$ be an algebraic series with $a(0) = 0$. Show that the compositional inverse of a is also algebraic.

18⋆. Is the series $\exp(x) \in C[[x]]$ algebraic?

19. Is the series $\arctan(x) \in \mathbb{C}[[x]]$ elementary?

20⋆. Show that $\log(x)$ is transcendental over $C((x))$, i.e., there is no polynomial $p \in C((x))[y] \setminus \{0\}$ such that $p(x, \log(x)) = 0$. Here $\log(x)$ is defined as a quantity whose derivative is $\frac{1}{x}$.

21. The function $\int \frac{1}{\log x} dx$ is not elementary. Show that it is differentially algebraic.

22⋆. Show that there is a unique formal power series $f \in \mathbb{Q}[[x]]$ with $f(0) = 1$ and

$$f(x) - f\Big(\frac{x^2}{4x-1}\Big) = \frac{\sqrt{1-4x}(x-1) - 3x + 1}{2x^2} = x + 3x^2 + 9x^3 + \cdots .$$

Compute its first few coefficients.

References

Rigorous developments of the theory of formal power series, which is only sketched in this section, can be found in many places: in [338], in Chapter 1 of [235], in Chapter 2 of [456], in Chapter 7 of [223], or in Chapter 2 of [268]. Also, the literature on computation is obviously vast. Classical texts on algorithms include [164, 279, 280, 401].

An overview of several classes of sequences and power series is given in [268]. A more detailed coverage of rational series is available in Chapter 4 of [413]. Classical texts on the deep subject of algebraic functions include [70, 146]. The result that every polynomial equation has a complete set of Puiseux series solutions appears for instance as Thm. 15.2 in [70]. The fact that the set of algebraic series forms a ring is discussed for instance in Sect. 6.4 of [268]. Hypergeometric series are discussed in detail in Chapters 2 and 3 of [32] and in Chapter 5 of [223]. Comprehensive fact collections are available in several chapters of [337] and [27].

Elementary functions have been studied intensively in the context of symbolic integration. The problem is to decide, for a given elementary function, whether its integral is again elementary. An algorithm was given in the 1960s by Risch [369, 370]. His algorithm is also described in [114] and in Chapter 12 of [206]. There are also algorithms for finding asymptotic expansions of elementary functions in terms of suitably generalized series, see [367, 404] and the references given there. Not all questions about elementary functions can be decided algorithmically though. Some undecidability results can be found in [366].

A short summary of facts about differentially algebraic functions is given in Sect. 6.1 of [57] and in a paper of Manssour, Sattelberger, and Teguia Tabuguia [320]. Denef and Lipshitz [170] discuss formal power series solutions of algebraic differential equations. They propose an algorithm for deciding whether a given algebraic differential equation has a power series solution. Algorithms for doing arithmetic with differentially algebraic functions mostly rely on the theory of Gröbner bases [47, 117, 167]. For example, see [403, 434] for algorithms that decide whether two given differentially algebraic functions are equal. For algebraic differential equations of order 1, there are algorithms for finding rational [193, 194] or algebraic [38] solutions.

Most computer algebra systems provide general purpose commands for "simplifying" expressions. Such commands are extremely useful, but it should not be misunderstood that they would accept arbitrary analytic functions or formal power series as input. Every such command, and every special purpose package for doing computations with formal power series, such as [282], applies to a certain class of series only, even if it is not clearly specified to which.

1.2 D-Finiteness

The class of D-finite functions is interesting for various reasons. First, the class is large enough that it covers a lot of functions that are of interest in different areas of mathematics, physics, and engineering. Second, the class is small enough that one can formulate (and implement, and execute) algorithms for answering questions about them. Third, the concept of D-finiteness is easily explained: in its most simple form, the definition just says that a function is D-finite if it is the solution to an ordinary linear differential equation with polynomial coefficients.

Definition 1.6

1. A formal Laurent series $f \in C((x))$ is called *differentially finite* or *D-finite* if there exist polynomials $p_0, \ldots, p_r \in C[x]$, with p_r not the zero polynomial, such that

$$p_0(x)f(x) + p_1(x)f'(x) + \cdots + p_r(x)f^{(r)}(x) = 0. \tag{1.1}$$

2. A meromorphic function $f : U \to \mathbb{C}$ defined on some open subset U of $\mathbb{C}$ is called *differentially finite* or *D-finite* if there exist polynomials $p_0, \ldots, p_r$, with p_r not the zero polynomial, such that

$$p_0(z)f(z) + p_1(z)f'(z) + \cdots + p_r(z)f^{(r)}(z) = 0$$

for all $z \in U$. □

Thus, for example, the exponential function exp is obviously D-finite (take $r = 1$, $p_0 = -1$, $p_1 = 1$ to get an appropriate equation), and so are sine and cosine, all rational functions, the square root function $z \mapsto \sqrt{z}$ (with $r = 1$, $p_0 = -1$, $p_1 = 2x$), in fact all algebraic functions (cf. Theorem 3.29 in Sect. 3.3), log (with $r = 2$, $p_0 = 0$, $p_1 = 1$, $p_2 = x$), a large number of special functions such as the n-th Bessel function J_n (with $r = 2$, $p_0 = x^2 - n^2$, $p_1 = x$, $p_2 = x^2$), various families of orthogonal polynomials such as the Legendre polynomials P_n (with $r = 2$, $p_0 = -n^2 - n$, $p_1 = 2x$, $p_2 = x^2 - 1$), and many other functions that arise in a variety of different contexts. An obvious example for a function that is not D-finite is the absolute value function $z \mapsto |z|$, because the definition applies only to functions which are sufficiently often differentiable. Less obvious examples include $z \mapsto \mathrm{e}^{\mathrm{e}^z}$ (Exercise 5), $z \mapsto 1/\log(z)$ (Exercise 18 in Sect. 3.3), and $z \mapsto \sqrt{\sin(z)}$

(Exercise 7 in Sect. 3.2). We have stated Definition 1.6 only for formal Laurent series and for meromorphic functions, but it applies more generally to any objects for which addition, differentiation, and multiplication by polynomials are meaningful operations.

Faced with a differential equation like (1.1), a typical question is whether some or all of its solutions can be expressed in a closed form. In almost all cases the answer is *no*. Only in very special circumstances can a D-finite function be written as a closed-form expression. Algorithms that can construct all closed form solutions for a given linear differential equation with polynomial coefficients are known, and we will discuss some of these algorithms in Sects. 3.5 and 3.6. But closed forms are only a small part of the story. We will see that many questions about D-finite functions can be answered algorithmically even if no closed form representation is available. Algorithms can use the differential equation rather than some explicit closed form expression as a data structure for representing a D-finite function. Observe that, at least if $p_r(0) \neq 0$, a solution f of (1.1) is uniquely determined by $f(0), f'(0), \dots, f^{(r-1)}(0)$, so these values together with the coefficients $p_0, \dots, p_r$ of the differential equation can be used to encode the D-finite function f.

In many ways, the theory of D-finite functions and series parallels the theory of algebraic functions and series. Recall that a series $f \in C((x))$ is called algebraic if there exists a nonzero bivariate polynomial p such that $p(x, f(x)) = 0$. In other words, f is algebraic if and only if there are univariate polynomials $p_0, \dots, p_r \in C[x]$, with p_r not the zero polynomial, such that

$$p_0(x) + p_1(x)f(x) + \cdots + p_r(x)f(x)^r = 0.$$

Some algebraic series can be written in terms of nested radical expressions, but most of them cannot. Nevertheless, much can be said about any particular algebraic series based on the polynomial equation it satisfies. In particular, if f is an algebraic series, then it is well-known and easy to show that the vector space generated by the powers $1, f, f^2, f^3, \dots$ of f over the field $C(x)$ of rational functions in one variable has a finite dimension, and the dimension is in fact the smallest $r \in \mathbb{N}$ such that f is *annihilated*, i.e., mapped to zero, by a polynomial $p \in C[x, y]$ whose degree in y is r. The corresponding statement for a D-finite series is as follows.

Proposition 1.7 *(Confinement property) A series $f \in C((x))$ is D-finite if and only if the vector space*

$$V(f) := C(x)f + C(x)f' + C(x)f'' + \cdots$$

generated by f and all of its derivatives over the field $C(x)$ of rational functions has finite dimension. If f is D-finite and r is the smallest number such that f satisfies an equation of the form (1.1)*, then $r = \dim_{C(x)} V(f)$.* □

Proof Suppose f is D-finite. Then f satisfies an equation of the form (1.1), say of order n. Let $V_n(f) := C(x)f + \cdots + C(x)f^{(n-1)}$ be the vector space generated by the first $n-1$ derivatives of f. We show that $V(f) \subseteq V_n(f)$. This then implies that

$\dim_{C(x)} V(f) \leq \dim_{C(x)} V_n(f) \leq n < \infty$. We show by induction that $f^{(i)} \in V_n(f)$ for all $i \geq 0$. For $i \leq n$ this is obvious. Now let $i \in \mathbb{N}$ be arbitrary and suppose that for all $j < i$ we have $f^{(j)} \in V_n(f)$. The differential equation assumed for f, differentiated $i-n$ times, allows us to express $f^{(i)}$ as a $C(x)$-linear combination of $f, f', \ldots, f^{(n-1)}, f^{(n)}, \ldots, f^{(i-1)}$. By the induction hypothesis, all of these terms belong to $V_n(f)$, and therefore $f^{(i)}$ also belongs to $V_n(f)$.

For the converse, suppose that $d := \dim_{C(x)} V(f)$ is finite. To show that f is D-finite it suffices to observe that any choice of $d+1$ vectors in a vector space of dimension d must be linearly dependent. We therefore have that there exist rational functions $q_0, \ldots, q_d \in C(x)$, not all zero, such that

$$q_0(x)f(x) + \cdots + q_d(x)f^{(d)}(x) = 0.$$

Clearing denominators, if necessary, leads to an equation of the form (1.1) for some $r \leq d$. Thus, f is D-finite.

It remains to address the claim about the smallest order r of an equation for f. The above arguments show that on the one hand we have $\dim_{C(x)} V(f) \leq n$ whenever f satisfies an equation of order n. In particular, $\dim_{C(x)} V(f) \leq r$. On the other hand, f always satisfies an equation of order $d = \dim_{C(x)} V(f)$, thus $r \leq \dim_{C(x)} V(f)$. This completes the proof. ■

A great part of the theory of D-finite functions rests on the confinement property formulated in this proposition. In fact, the 'finite' in the word D-finite refers to the fact that $V(f)$ has a finite dimension. The 'D' refers to the fact that V is constructed by <u>d</u>ifferentiating f, rather than, say, by taking powers.

Note that $V(f)$ is not only closed under taking linear combinations with coefficients in $C(x)$ but also under taking derivatives, for if

$$g(x) = q_0(x)f(x) + \cdots + q_{r-1}(x)f^{(r-1)}(x)$$

is an arbitrary element of $V(f)$, then

$$\begin{aligned}
g'(x) &= \big(q_0'(x)f(x) + q_0(x)f'(x)\big) + \cdots + \big(q_{r-1}'(x)f^{(r-1)}(x) + q_{r-1}(x)f^{(r)}(x)\big) \\
&= q_0'(x)f(x) + \big(q_0(x) + q_1'(x)\big)f'(x) + \cdots + \big(q_{r-2}(x) + q_{r-1}'(x)\big)f^{(r-1)}(x) \\
&\qquad + q_{r-1}(x)f^{(r)}(x)\big) \\
&= \Big(q_0'(x) - \frac{q_{r-1}p_0(x)}{p_r(x)}\Big)f(x) + \cdots \\
&\qquad + \Big(q_{r-2}(x) + q_{r-1}'(x) - \frac{q_{r-1}p_{r-1}(x)}{p_r(x)}\Big)f^{(r-1)}(x)
\end{aligned}$$

also belongs to $V(f)$. Indeed, $V(f)$ is the smallest $C(x)$-vector space that contains f and is closed under differentiation. The calculation above becomes more transparent when formulated in terms of matrix-vector multiplication. The differential equation for f can be rephrased as

$$\begin{pmatrix} f' \\ f'' \\ \vdots \\ \vdots \\ f^{(r)} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \cdots & 0 \\ \vdots & 0 & \ddots \ddots & \vdots \\ \vdots & \vdots & \ddots \ddots & 0 \\ 0 & 0 & \cdots 0 & 1 \\ -p_0/p_r & -p_1/p_r & \cdots\cdots & -p_{r-1}/p_r \end{pmatrix} \begin{pmatrix} f \\ f' \\ \vdots \\ \vdots \\ f^{(r-1)} \end{pmatrix}.$$

The matrix appearing in this equation is called the *companion matrix* of the differential equation for f. If we write P for the companion matrix and $\bar{f} = (f, \ldots, f^{(r-1)})^T$, so that $\bar{f}' = P\bar{f}$, then every element $g(x) = q_0(x)f(x) + \cdots + q_{r-1}(x)f^{(r-1)}(x)$ of $V(f)$ can be represented by a vector $\bar{g} = (q_0, \ldots, q_{r-1}) \in C(x)^r$. By the product rule, we have $g' = (\bar{g}\bar{f})' = \bar{g}'\bar{f} + g\bar{f}' = (\bar{g}' + \bar{g}P)\bar{f}$, where $\bar{g}' = (q_0', \ldots, q_{r-1}')$. Thus, g' is represented by the vector $\bar{g}' + \bar{g}P$.

Some properties of D-finite functions follow immediately from the confinement property. For example, if f and g are two D-finite functions, then $V(f)$ and $V(g)$ have finite dimension, so the sum $V(f) + V(g)$ of these subspaces also has finite dimension. Since this sum contains $f + g$ and all of its derivatives, it contains the subspace $V(f + g)$, which therefore also has finite dimension. This proves that the sum of D-finite functions is D-finite, one of many closure properties that the class of D-finite functions enjoys. We will see more of them in Sects. 2.3 and 3.3.

The confinement property may also work for other operations besides the derivative. Other operations lead to classes of functions which enjoy very similar structural properties as the class of D-finite functions as defined in Definition 1.6. For example, we can consider recurrence equations instead of differential equations. In this case, the shift operator $f(z) \rightsquigarrow f(z+1)$ plays the role of the derivation.

Definition 1.8 Let $A \subseteq C$ be such that $\forall\, z \in A : z+1 \in A$. A function $f\colon A \to C$ is called *D-finite* (also: *P-finite* or *P-recursive*) if there exist polynomials $p_0, \ldots, p_r$, with p_r not the zero polynomial, such that

$$p_0(z)f(z) + p_1(z)f(z+1) + \cdots + p_r(z)f(z+r) = 0 \tag{1.2}$$

for all $z \in A$. □

Examples for functions which are D-finite in the sense of this definition include rational functions, the gamma function Γ, the digamma function ψ, periodic functions such as $z \mapsto \sin(\pi z)$ and $z \mapsto \cos(\pi z)$, and many others. It must be observed that D-finiteness as defined in Definition 1.6 is not equivalent to D-finiteness as defined in Definition 1.8. For example, the gamma function is not D-finite in the sense of Definition 1.6. To be more precise, we should say that a function such as $z \mapsto \sqrt{z}$ is D-finite *with respect to derivation* whereas a function such as Γ is D-finite *with respect to shift.*

Usually there will be no confusion because we will almost always use Definition 1.6 for functions that depend on a "continuous" argument and Definition 1.8 only for functions whose argument is regarded as "discrete", viz. sequences. Examples include the sequence of Fibonacci numbers F_n, the harmonic numbers $H_n = \sum_{k=1}^{n} \frac{1}{k}$, Catalan numbers $C_n = \frac{1}{n+1}\binom{2n}{n}$, and many other sequences that appear in combinatorics.

If p_r does not have a positive integer root, then every sequence solution $f : \mathbb{N} \to C$ of (1.2) is uniquely determined by its initial values $f(0), \dots, f(r-1)$, and conversely, every choice of initial values gives rise to a sequence solution. More generally, if p_r does have integer roots, a solution $f : \mathbb{N} \to C$ is still uniquely determined by the initial values $f(0), \dots, f(r-1)$ together with the values $f(s+r)$ for every positive integer root s of p_r. However, in this general situation it is not true that for every choice of initial values $f(0), \dots, f(r-1)$ there does exist a corresponding sequence solution of (1.2). We will have a closer look at this phenomenon in Chap. 2, where we discuss D-finite sequences in detail.

For the time being, let us formulate a sequence analog of Proposition 1.7. This requires some care, because the set of all sequences $\mathbb{N} \to C$ does not naturally form a vector space over the field $C(x)$ of rational functions. We would like to embed $C(x)$ into the ring of sequences by mapping a rational function p/q to the sequence $z \mapsto p(z)/q(z)$, but this fails for rational functions whose denominators have positive integer roots. One possibility is to consider a $C[x]$-module instead of a $C(x)$-vector space, but then we leave the realm of linear algebra. Another possibility is to consider germs of sequences, defined as follows. For simplicity, we restrict to the case $A = \mathbb{N}$.

Definition 1.9 Two sequences $f, g \in C^{\mathbb{N}}$ are said to be equivalent, written $f \sim g$, if there exists a finite set $E \subseteq \mathbb{N}$ such that for all $n \in \mathbb{N} \setminus E$ we have $f(n) = g(n)$. The elements of $C^{\mathbb{N}}/_{\sim}$ are called *germs of sequences.* □

It is easy to see that $\sim$ is indeed an equivalence relation, and that it is compatible with termwise addition and multiplication, so that $C^{\mathbb{N}}/_{\sim}$ inherits the natural ring structure of $C^{\mathbb{N}}$. The field $C(x)$ can be embedded into $C^{\mathbb{N}}/_{\sim}$ because for every rational function $p/q \in C(x)$ there exist only finitely many points $n \in \mathbb{N}$ with $q(n) = 0$. We can therefore take E as the set of integer roots of q and map p/q to any sequence $f : \mathbb{N} \to C$ with arbitrary values $f(n)$ for $n \in E$ and with $f(n) = p(n)/q(n)$ for $n \in \mathbb{N} \setminus E$. The shift operation is also well-defined on $C^{\mathbb{N}}/_{\sim}$: if $[f]$ is the equivalence class of a sequence $f : \mathbb{N} \to C$, then we define $S([f]) := [g]$ where $g : \mathbb{N} \to C$ is defined by $g(n) := f(n+1)$ for all $n \in \mathbb{N}$. A germ $f \in C^{\mathbb{N}}/_{\sim}$ is called D-finite if there exist polynomials $p_0, \dots, p_r \in C[x]$ with p_r not the zero polynomial such that the equation

$$p_0 f + p_1 S(f) + \cdots + p_r S^r(f) = 0 \tag{1.3}$$

holds in $C^{\mathbb{N}}/_{\sim}$. In this setting, the sequence version of the confinement property can be formulated as follows.

Proposition 1.10 *A germ of sequences $f \in C^{\mathbb{N}}/_{\sim}$ is D-finite if and only if the vector space*

$$V(f) := C(x)f + C(x)S(f) + C(x)S^2(f) + \cdots \quad \subseteq C^{\mathbb{N}}/_{\sim}$$

generated by f and all of its shifts $S^i(f)$ ($i \in \mathbb{N}$) over the field $C(x)$ has finite dimension.

If f is D-finite and r is the smallest number such that f satisfies an equation of the form (1.3), then $r = \dim_{C(x)} V(f)$. □

Proof Exercise 10. ■

Working with germs can often lead to simpler proofs and more elegant theoretical statements, but it must be observed that applications typically require statements about actual sequences $f : \mathbb{N} \to C$ rather than about germs. If we want to prove some identity $\forall\, n \in \mathbb{N} : f(n) = g(n)$, then it is not too helpful if we do a calculation with germs which only implies that $f(n) = g(n)$ is true "for all except for finitely many $n \in \mathbb{N}$" without telling us what the finitely many possible exceptional points are. On the other hand, we can easily complete the proof by checking whether $f(n) = g(n)$ holds for these finitely many points, if they are known.

In Chap. 2, we will consider linear recurrence equations with polynomial coefficients in great detail. Afterwards, in Chap. 3, we discuss analogous techniques for the case of linear differential equations. Although there are subtle differences throughout, most of the results in one chapter have a counter part in the other chapter. Some features are literally identical when they are formulated in terms of linear operators.

Writing D for the differential operator that maps a function f to its derivative f', we can rephrase Definition 1.6 by saying that f is D-finite if there exists a nonzero operator

$$L = p_0 + p_1 D + \cdots + p_r D^r$$

such that $L \cdot f = 0$ (read: "L applied to f is zero" or "L annihilates f"). Similarly, writing S for the shift operator acting on sequences (or germs of sequences), Definition 1.9 says that f is D-finite if there exists a nonzero operator

$$L = p_0 + p_1 S + \cdots + p_r S^r$$

such that $L \cdot f = 0$. In both cases, if p_r is not zero, we call r the *order* of the operator.

In Chap. 4 we will introduce a general type of linear operators, which includes differential operators and recurrence operators as special cases. These operators, known as Ore polynomials, have the form

$$p_0 + p_1 \partial + \cdots + p_r \partial^r$$

where $p_0, \dots, p_r$ are rational functions in x and ∂ is a formal indeterminate that could stand for D or S. The set of all these operators will be denoted by $C(x)[\partial]$. It is the $C(x)$-vector space generated by $1, \partial, \partial^2, \dots$.

If F is another $C(x)$-vector space, such as the space of all meromorphic functions on a certain Riemann surface (if $C = \mathbb{C}$), or the field $C((x))$ of formal Laurent series, or the ring $C^{\mathbb{N}}/\sim$ of germs of sequences, we will turn F into a $C(x)[\partial]$-(left-) module in which ∂ acts like the derivative or the shift, for example. Multiplication of operators is defined in such a way that it is compatible with this action, i.e., so that $(ML) \cdot f = M \cdot (L \cdot f)$ for all $M, L \in C(x)[\partial]$ and all $f \in F$. In general, this multiplication will be noncommutative, and the precise type of non-commutativity is governed by ∂. For example, in the differential case we have $\partial x = x\partial + 1$, because $(xf)' = xf' + f$, and in the recurrence case we have $\partial x = (x+1)\partial$, because $S(xf) = (x+1)S(f)$.

For every fixed $f \in F$, there is a canonical morphism $\phi\colon C(x)[\partial] \to F$ with $\phi(1) = f$. By the homomorphism theorem, we have

$$C(x)[\partial]/\ker\phi \cong \operatorname{im}\phi = V(f)$$

as $C(x)[\partial]$-(left-)modules. The element f is D-finite if the left-ideal $\ker\phi$ is nonempty, and this is the case if and only if $C(x)[\partial]/\ker\phi$ is a finite-dimensional $C(x)$-vector space. This is the confinement property from Propositions 1.7 and 1.10 in the language of operator algebras.

Sect. 4.5 is about D-finiteness for functions in several variables. In order to get the confinement property for functions in this case, it is not enough to require a single differential or recurrence equation with polynomial coefficients. In fact, instead of saying explicitly which equations are required, it seems more elegant to use the confinement property itself as a definition.

Definition 1.11 Let $C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n]$ be an algebra of operators in which the ∂_i commute with each other (but not necessarily with elements from the ground field; see Sect. 4.5 for a detailed discussion). Let F be a $C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n]$-left-module. Let $f \in F$, and let

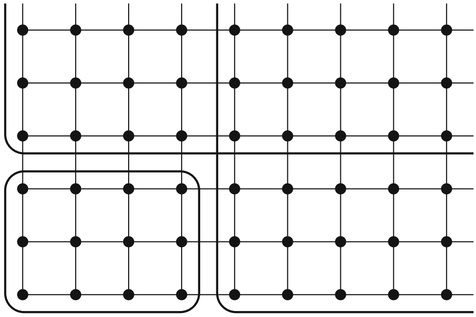
$$\phi\colon C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n] \to F$$

be the canonical morphism with $\phi(1) = f$. The element f is called *D-finite* if

$$C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n]/\ker\phi$$

is a finite-dimensional vector space over $C(x_1, \dots, x_n)$. □

An equivalent way of phrasing this definition is to say that f is D-finite if the $C(x_1, \dots, x_n)$-subspace generated by all of the elements $\partial_1^{e_1} \cdots \partial_n^{e_n} \cdot f$ in F has finite dimension. One way to ensure this condition is to require that for every $i \in \{1, \dots, n\}$, there is a nonzero operator $L \in C(x_1, \dots, x_n)[\partial_i]$ such that $L \cdot f = 0$. For example, in the case of $n = 2$ variables, if $f \in F$ is an object that has an annihilating operator of order 5 in $C(x_1, x_2)[\partial_1]$ and an annihilating operator of order 4 in $C(x_1, x_2)[\partial_2]$, the vector space is generated by $\partial_1^i \partial_2^j \cdot f$ with $i = 0, \dots, 4$ and $j = 0, \dots, 3$. By the assumed annihilating operators, every other term $\partial_1^i \partial_2^j$ is equivalent to a certain $C(x_1, x_2)$-linear combination of those.



In the setting of Definition 1.11, the ∂_i may act like partial derivations on meromorphic functions or formal Laurent series in several variables. In this case, we use an algebra $C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n]$ in which the multiplication is governed by the commutation rules $\partial_i x_i = x_i \partial_i + 1$ $(i = 1, \dots, n)$, $\partial_i x_j = x_j \partial_i$ $(i \neq j)$, and $\partial_i \partial_j = \partial_j \partial_i$ $(i, j = 1, \dots, n)$.

Example 1.12 The function $f : \mathbb{C}^2 \to \mathbb{C}$, $f(x, y) = \exp(1 - xy) + \exp(x - y^2)$ is D-finite with respect to x and y because it satisfies the two equations

$$\big(y - (y - 1)D_x - D_x^2\big) \cdot f = 0,$$
$$\big(2x(1 + xy - 2y^2) + (2 + x^2 - 4y^2)D_y + (x - 2y)D_y^2\big) \cdot f = 0.$$

Note that the first equation involves only derivations with respect to x while the second has only derivations with respect to y. There is no such restriction on the polynomial coefficients: x and y are both allowed to occur in the coefficients of any equation. □

Besides equations involving only one partial derivation, D-finite functions satisfy many other equations. For example, the function f in the example above also satisfies the partial differential equation

$$\big((x + 2y^2) + (2y - x)D_x + (1 + y)D_y\big) \cdot f = 0,$$

which involves both a derivative with respect to x and a derivative with respect to y. All such equations need to be taken into account if we want to accurately describe the vector space $V(f)$ generated by all of the partial derivatives $D_x^i D_y^j \cdot f$ over the field $C(x, y)$ of rational functions in x and y. But for merely checking the confinement property, it suffices to have one operator for each ∂_i. These are sometimes called *pure operators.*

Before we can cover sequences in several variables, we need to address again the problem that the rational function field $C(x_1, \dots, x_n)$ does not directly admit an embedding into the ring $C^{\mathbb{N}^n}$ of multivariate sequences, because rational functions may have poles at some point with positive integer coordinates. The problem can be repaired essentially like before, if we reformulate the definition of germs in such a way that it accounts for the fact that multivariate polynomials may have infinitely many roots.

Definition 1.13 Two sequences $f, g \in C^{\mathbb{N}^n}$ are said to be equivalent, $f \sim g$, if there exists a polynomial $p \in C[x_1, \dots, x_n]\setminus\{0\}$ such that for all $(k_1, \dots, k_n) \in \mathbb{N}^m$ we have $p(k_1, \dots, k_n) = 0$ or $f(k_1, \dots, k_n) = g(k_1, \dots, k_n)$. The elements of $C^{\mathbb{N}^n}/\sim$ are called *germs of sequences.* □

We can let an algebra $C(x_1, \dots, x_n)[\partial_1, \dots, \partial_n]$ of Ore polynomials with the commutation rules $\partial_i x_i = (x_i + 1)\partial_i$ $(i = 1, \dots, n)$ and $\partial_i x_j = x_j \partial_i$ $(i \neq j)$ act on the set of germs in such a way that each ∂_i serves as a shift operation for the ith index of the sequence. It is also possible to consider mixed situations with some continuous and some discrete variables.

Example 1.14

1. The binomial coefficient $\binom{n}{k}$ is D-finite with respect to n and k because it satisfies the two equations
$$\big((1+n) - (1-k+n)S_n\big) \cdot \binom{n}{k} = 0 \quad \text{and} \quad \big((k-n) + (k+1)S_k\big) \cdot \binom{n}{k} = 0,$$
where we write S_n, S_k instead of ∂_1, ∂_2 for the shift operators with respect to n and k, respectively. Note that the first recurrence is pure in S_n and the second is pure in S_k.
2. The Legendre polynomials $P_n(x)$ are D-finite with respect to x and n because they satisfy the equations
$$\big((n+1) - (2nx + 3x)S_n + (n+2)S_n\big) \cdot P_n(x) = 0,$$
$$\big((-n - n^2) + 2xD_x + (x^2 - 1)D_x^2\big) \cdot P_n(x) = 0.$$

□

Thanks to the confinement property, many facts about univariate D-finite functions generalize naturally to multivariate D-finite functions. And even more can be done. Of particular importance is the case of definite summation and integration, which we shall discuss in detail in Chap. 5. We will see there that if $f(x, y)$ is D-finite as a bivariate complex function, then so is the univariate function $F(x) := \int_\Omega f(x, y)dy$, where Ω is a suitable domain of integration. It is possible to compute a differential equation satisfied by the integral $F(x)$ given a system of defining equations for the integrand $f(x, y)$. Similarly, if $f(n, k)$ is a sufficiently well-behaved bivariate D-finite sequence, the definite sum $F(n) = \sum_{k=0}^{n} f(n, k)$ will again be D-finite, and we can compute a recurrence equation satisfied by the sum $F(n)$ given a system of defining recurrence equations for the summand $f(n, k)$.

Exercises

1⋆. Suppose that a univariate function f satisfies an inhomogeneous differential equation

$$p_0(x)f(x) + p_1(x)f'(x) + \cdots + p_r(x)f^{(r)}(x) = q(x)$$

where $p_0, \ldots, p_r$ as well as the inhomogeneous part q are in $C[x]$ and p_r is not the zero polynomial. Show that f is D-finite.

2⋆. Show that arcsin, arccos, arctan are D-finite, while tan is not D-finite.

3. Let f be a solution of $(x + 1)f + (2x + 3)f' + (4x + 5)f'' = 0$. Express $f^{(5)}$ as a linear combination of f and f' with rational function coefficients.

4. Show that $H_n = \sum_{k=1}^{n} \frac{1}{k}$ is D-finite and that 2^{2^n} is not.

5. Show that $\mathrm{e}^{\mathrm{e}^z}$ is not D-finite.
Hint: You may use that e^z is not algebraic (cf. Exercise 18 in Sect. 1.1).

6. Show that the sequence $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = |n|$ is D-finite.

7. Let $f = \sum_{n=0}^{\infty} a_n x^n$ be a formal power series. Show that f is D-finite with respect to derivation if and only if $(a_n)_{n=0}^{\infty}$ is D-finite with respect to shift.

8. For two sequences $f, g \in C^{\mathbb{N}}$, define

$$f \equiv g \quad :\Longleftrightarrow \quad \exists\, n_0 \in \mathbb{N}\; \forall\, n > n_0 : f(n) = g(n).$$

Show that $f \equiv g \iff f \sim g$.

9⋆⋆. Show that a germ of sequences is D-finite if and only if all of its elements are D-finite as univariate sequences.

10⋆. Prove Proposition 1.10.

11. Prove or disprove: If a D-finite function f satisfies a differential equation

$$p_1 f' + \cdots + p_r f^{(r)} = 0$$

with $p_1, \ldots, p_r \in C[x]$ and $p_r \neq 0$, then it also satisfies a differential equation of order less than r.

12. Prove or disprove: If a D-finite sequence $f: \mathbb{N} \to C$ satisfies a recurrence

$$p_1(n)f(n+1) + \cdots + p_r(n)f(n+r) = 0$$

with $p_1, \ldots, p_r \in C[x]$ and $p_r \neq 0$, then it also satisfies the recurrence

$$p_1(n-1)f(n) + \cdots + p_r(n-1)f(n+r-1) = 0.$$

Does the situation change if we consider germs of sequences, or sequences $f: \mathbb{Z} \to C$?

13. Let $f \in C^{\mathbb{N}}/\sim$ be D-finite, and let P be the companion matrix of a recurrence equation satisfied by f. If we represent an element $g = q_0 f + q_1 S(f) + \cdots + q_{r-1}S^{r-1}(f)$ of $V(f)$ by a vector $v = (q_0, \ldots, q_{r-1}) \in C(x)^r$, what is the vector corresponding to $S(g)$?

14. Show that $\ker \phi$ is a left-ideal of $C(x)[\partial]$.

15. Consider the differential operator $L = (2x-1) - (4x^2 - 8x + 5)\partial + (4x^2 - 10x + 6)\partial^2$ in the algebra $C(x)[\partial]$ with the commutation rule $\partial x = x\partial + 1$. Check that $L \cdot \sqrt{1-x} = 0$. Then find a first-order differential operator $V \in C(x)[\partial]$ with $V \cdot \sqrt{1-x} = 0$ and use it to write L as a product $L = UV$ for some other first-order operator $U \in C(x)[\partial]$.

16.** Show that the two recurrence equations

$$(n+k)f(n,k) - (2n+3k)f(n,k+1) = 0, \quad (4n+5k)f(n,k) - f(n+1,k) = 0$$

have no nontrivial common solution.

17.** Show that every function f which satisfies the two equations

$$(x+2y^2)f + (2y-x)\frac{\partial}{\partial x}f + (1+y)\frac{\partial}{\partial y}f = 0,$$
$$yf - (y-1)\frac{\partial}{\partial x}f - \frac{\partial^2}{\partial x^2}f = 0$$

is D-finite.

18. **a.** Show that the relation $\sim$ in Definition 1.13 is indeed an equivalence relation. **b.** Show that the case $m = 1$ of Definition 1.13 is equivalent to Definition 1.9.

19.** Let $f: \mathbb{N}^2 \to C$ be such that for every fixed $n \in \mathbb{N}$ the univariate sequence $f(n, \cdot)$ is D-finite, and for every fixed $k \in \mathbb{N}$ the univariate sequence $f(\cdot, k)$ is D-finite. Does this imply that f is D-finite as a bivariate sequence?

References

The notion of D-finiteness was coined by Stanley in [412], where he points out that a wide range of combinatorial objects have D-finite generating functions. Although the significance of linear recurrences and differential equations was recognized long before (see, for example, Schlesinger's handbook on linear differential equations [381–383] for the state of the art almost a hundred years earlier), Stanley observes that many of the basic facts get rediscovered from time to time. One goal of his paper was therefore to put the basic facts about D-finite power series together into a unified theory. His discussion also covers D-finite sequences (which he calls "P-recursive").

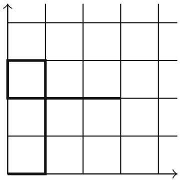
The coverage of multivariate functions goes back to Zeilberger's paper [466]. In his later paper [468], he uses the word P-finite instead of D-finite for both the differential as well as the recurrence case, and he also introduces the word C-finite for functions/sequences satisfying differential/recurrence equations with constant coefficients. He also talks about holonomy, a concept which is closely related to D-finiteness. We shall discuss the subtle differences in Sect. 4.5.

Most of the material in this section will be discussed in greater depth in later sections, and specialized references will be given there. For shorter overviews of the main results, see also the surveys [264, 266, 378].

1.3 Applications

In this book we discuss D-finite functions primarily from the algorithmic point of view. We will see which problems about D-finite functions can be solved automatically, and how this works. The focus is not so much on why we might want to solve these problems at all. It must be emphasized however that the intensive development of algorithms for D-finite functions during the past decades was not only caused by scientific curiosity. Instead, the algorithmic development responds to demands from other areas in which D-finite functions arise naturally. Algorithms for D-finite functions find nowadays applications in such diverse contexts that a comprehensive coverage of these applications could easily fill a separate book. In this section, we will just give a glimpse of the possibilities. To see the machinery of D-finite functions in action, we only discuss an application from enumerative combinatorics in some detail. Afterwards we briefly comment on further application areas.

For any $n \in \mathbb{N}$, define a_n as the number of all lattice walks in $\mathbb{N}^2$ that start at the origin and consist of n steps, each step being one of $\uparrow$, $\downarrow$, $\leftarrow$, or $\rightarrow$. Observe that the walk is restricted to the nonnegative quadrant. Here is an example for such a walk:



It is not hard to compute the first few terms of the sequence $(a_n)_{n=0}^{\infty}$. If we let $a_{n,i,j}$ be the number of walks of length n ending at (i, j), then the combinatorial specification translates into the recurrence

$$a_{n+1,i,j} = a_{n,i+1,j} + a_{n,i-1,j} + a_{n,i,j+1} + a_{n,i,j-1},$$

which along with the initial value $a_{0,0,0} = 1$ and the boundary conditions $a_{n,-1,j} = a_{n,i,-1} = 0$ uniquely determines the sequence $(a_{n,i,j})_{n,i,j=0}^{\infty}$. With $a_n = \sum_{i,j=0}^{n} a_{n,i,j}$, we obtain the first terms as

$$1, 2, 6, 18, 60, 200, 700, 2450, 8820, 31752, 116424.$$

Is this a D-finite sequence? Using the techniques from Sects. 1.5 and 1.6, we can construct plausible hypothesis for a recurrence equation or a differential equation for the corresponding power series. The terms listed above are not quite enough, but with the first 50 terms, we can effortlessly guess the recurrence equation

$$(n+3)(n+4)a_{n+2} - 4(2n+5)a_{n+1} - 16(n+1)(n+2)a_n \stackrel{?}{=} 0$$

for the sequence and the differential equation

$$\begin{aligned}(4t-1)(4t+1)t^2a^{(3)}(t) &+ 2(4t+1)(16t-3)ta''(t)\\ &+ 2(112t^2+14t-3)a'(t) + 4(16t+3)a(t) \stackrel{?}{=} 0\end{aligned}$$

for the generating function $a(t) = \sum_{n=0}^{\infty} a_n t^n$.

If these equations are correct, we can extract further information from them. For example, using the algorithms from Sects. 2.5 and 2.6, we can check whether the recurrence has certain closed form solution. It turns out that this is not the case. With the algorithms from Sects. 3.5 and 3.6, the analogous question can be answered for the differential equation, and the only closed form solution they find is $1/t$, which is obviously not equal to $a(t)$. The concept "closed form" has a somewhat vague nature. Some expressions may be acceptable as closed form solutions in certain contexts but not in others. Algorithms for finding closed form solutions of recurrences or differential equations always apply to very specific types of closed forms. The algorithms presented in Chaps. 2 and 3 are complete in the sense that if they do not find a closed form solution, then there definitely is no closed form of the respective type. It may still be possible to express the solutions by some other kind of closed form expression. For example, the guessed recurrence has the solution

$$\binom{n}{\lfloor n/2 \rfloor}\binom{n+1}{\lfloor (n+1)/2 \rfloor},$$

and the guessed differential equation has the solutions

$$t^{-1}{}_2F_1\Bigl(\begin{matrix}1/2, 1/2\\ 1\end{matrix} \Bigm| 16t^2\Bigr) \quad \text{and} \quad {}_2F_1\Bigl(\begin{matrix}1/2, 3/2\\ 2\end{matrix} \Bigm| 16t^2\Bigr).$$

While algorithms for *finding* such kinds of solutions are beyond the scope of this book, algorithms for *proving* the correctness of these solutions are covered in Sects. 2.3 and 3.3.

Instead of closed form expressions, we can ask for asymptotic information. The algorithm of Sect. 2.4 tells us that the guessed recurrence has the series solutions

$$\begin{aligned}(-4)^n n^{-3}\Bigl(1 - \frac{9}{2n} + \frac{107}{8n^2} - \frac{525}{16n^3} + \frac{9263}{128n^4} - \frac{38787}{256n^5} + \cdots\Bigr)\\ 4^n n^{-1}\Bigl(1 - \frac{3}{2n} + \frac{19}{8n^2} - \frac{63}{16n^3} + \frac{871}{128n^4} - \frac{3129}{256n^5} + \cdots\Bigr),\end{aligned}$$

which suggests that the sequence behaves asymptotically like $a_n \sim c4^n n^{-1}$ for a certain constant c. Using algorithms from Sect. 2.1 and the guessed recurrence, we can efficiently compute sequence terms for very large n. With such terms, we can estimate the multiplicative constant $c \approx a_n/(4^n n^{-1})$. Already for the moderate $n = 25000$ we obtain the estimate $c \approx 1.273$. Taking also some higher order terms of the asymptotic expansion into account, as explained in Example 2.36, we can get the better estimate

$$c \approx 1.2732395447351626861510701069801148962756771659236515899813 4.$$

Asymptotic information about the sequence can also be obtained from the guessed differential equation. According to the theory of analytic combinatorics, the asymptotic behaviour of a_n is determined by the singularities of $a(t)$ that are closest to the origin. The singularities of $a(t)$ are the roots of the coefficient of $a^{(3)}(t)$ in the differential equation, i.e., $1/4$ and $-1/4$ (the additional singularity at 0 is irrelevant). The algorithm of Sect. 3.4 tells us that at these points the differential equations has solutions with logarithmic singularities. The series expansions of these singular solutions can be translated into the asymptotic expansions obtained above from the recurrence.

Before we see how to prove that the two guessed equations are correct, let us show that each equation implies the other. Theorem 2.33 allows us to translate the guessed recurrence into the differential equation

$$(t^2-16t^4)a^{(4)}(t)+(-192t^3-8t^2+8t)a^{(3)}(t)+(-608t^2-44t+12)a''(t)$$
$$+(-512t-40)a'(t)-64a(t)=0.$$

The meaning of this translation is that every power series whose coefficient sequence is a solution of the guessed recurrence is a solution of this differential equation. Observe that the equation above is different from the differential equation we obtained via guessing. The relation between the two equations can be revealed using operator techniques from Chap. 4. Writing the guessed equation as $L_1 \cdot a(t) = 0$ and the equation above as $L_2 \cdot a(t) = 0$ for some differential operators L_1, L_2, Algorithm 4.17 shows that L_1 is a right factor of L_2, i.e., there is another differential operator Q such that $L_2 = QL_1$. It can be deduced from here that if a power series solution of L_2 and a power series solution of L_1 agree up to a certain finite order, then they must be identical. Using the so-called indicial polynomial (cf. Definition 3.34) it can be determined how many terms need to be compared. In our case, two terms are enough. It follows that every power series whose coefficient sequence starts with $1, 2, 6$ and satisfies the guessed recurrence must satisfy the guessed differential equation. Conversely, it can be shown by an analogous reasoning using Theorem 2.33 and Algorithm 4.17 that the coefficient sequence of every power series solution of the guessed differential equation starting with $1 + 2t + 6t^2 + \cdots$ must satisfy the guessed recurrence. So if one of the two guessed equations is correct, the other is correct too.

In order to prove the correctness of both equations, we take a detour through the trivariate sequence that carries additional information about the combinatorial problem. Recall that we denoted by $a_{n,i,j}$ the number of walks of length n that end at the point $(i, j) \in \mathbb{N}^2$, and define $a(x, y, t) = \sum_{n=0}^{\infty} \sum_{i,j=0}^{n} a_{n,i,j} x^i y^j t^n$ as the power series corresponding to this multivariate sequence. The recurrence we used above for computing the first few terms of the sequence along with its initial value and the applicable boundary conditions imply the functional equation

$$a(x, y, t) = 1 + t\bigl(x + y + \tfrac{1}{x} + \tfrac{1}{y}\bigr)a(x, y, t) - \tfrac{t}{x}a(0, y, t) - \tfrac{t}{y}a(x, 0, t).$$

On the right hand side, the term 1 encodes the initial condition $a_{n,0,0} = 1$, the second term on the right encodes the recurrence, and the last two terms encode the boundary conditions imposed by the two coordinate axes.

The guessing techniques of Sect. 1.5 also work in the multivariate setting, and they suggest that $a(x, y, t)$ is in fact D-finite in all three variables. The ideal of annihilating operators (cf. Sect. 4.5) appears to have a Gröbner basis (cf. Sect. 4.6) with leading terms $D_x^2, D_tD_y, D_tD_x, D_t^2, D_y^3, D_xD_y^2$. It can be shown that the solution space in $C[[x, y, t]]$ of this system of equations has exactly one power series solution with constant term 1, and it can further be shown that the functional equation for $a(x, y, t)$ has exactly one solution in $C[[x, y, t]]$. Therefore, in order to show that $a(x, y, t)$ is really D-finite, it suffices to show that the unique power series solution $\hat{a}(x, y, t)$ with constant term 1 of the guessed ideal of differential operators satisfies the functional equation.

This can be done using *closure properties* (Sects. 2.3, 3.3, 4.5, 5.3). First, using creative telescoping (Chap. 5) we can compute ideals of annihilating operators for $\hat{a}(0, y, t)$ and $\hat{a}(x, 0, t)$. Next, using techniques from Sect. 4.5, we can compute ideals of annihilating operators of $t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)\hat{a}(x, y, t)$, $\frac{t}{x}\hat{a}(0, y, t)$, and $\frac{t}{y}\hat{a}(x, 0, t)$, respectively, and from these, an ideal of annihilating operators for $1 + t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)\hat{a}(x, y, t) - \frac{t}{x}\hat{a}(0, y, t) - \frac{t}{y}\hat{a}(x, 0, t)$. Using Gröbner bases technology (Sect. 4.6), we can then show that this ideal is consistent with the ideal for $\hat{a}(x, y, t)$, generalizing the reasoning we outlined before for checking the consistency of the univariate operators L_1 and L_2. The conclusion is then that $a(x, y, t) = \hat{a}(x, y, t)$, i.e., that $a(x, y, t)$ is D-finite. The ideal of annihilating operators for $a(x, y, t)$ must contain an operator that only involves x, y, t, D_t but not D_x or D_y, and Gröbner bases can find such an operator. Setting $x = y = 1$ in this operator yields an annihilating operator for $a(t) = a(1, 1, t)$. This completes the proof that $a(t)$ is D-finite. The operator L_3 obtained in this way is not the operator L_1 we directly found for $a(t)$ by guessing, but again an operator of higher order. To finally show that L_1 is correct, we use again Algorithm 4.17 to show that L_1 is a right factor of L_3 and check a few initial values.

The proof strategy just described is guaranteed to succeed in theory, but it might not work in practice owing to the required amount of computation. In order to reduce the computational cost to a more reasonable amount, we need to invest some more thought. A good idea is to reduce the number of variables involved. This can be done as follows. Rewrite the functional equation as

$$\Big(1 - t\big(x + y + \tfrac{1}{x} + \tfrac{1}{y}\big)\Big)a(x, y, t) = 1 - \tfrac{t}{x}a(0, y, t) - \tfrac{t}{y}a(x, 0, t).$$

One of the roots of the Laurent polynomial $1 - t\big(x + y + \frac{1}{x} + \frac{1}{y}\big) \in C(t, x)[y, y^{-1}]$ appearing on the left is a power series $Y \in C(x)[[t]]$ whose first terms are

$$t + (x + \tfrac{1}{x})t^2 + (\tfrac{1}{x^2} + 3 + x^2)t^3 + \cdots .$$

Substituting this power series into the functional equation gives $0 = 1 - \frac{t}{x}a(0, Y, t) - \frac{t}{Y}a(x, 0, t)$, which we can rewrite to

$$a(x, 0, t) = \tfrac{Y}{t} - \tfrac{Y}{x}a(Y, 0, t),$$

taking into account that $a(x, y, t)$ is symmetric with respect to x and y. Note that this new functional equation no longer involves y but only contains the variables x and t. We can now guess a D-finite system of annihilating operators for $a(x, 0, t)$ and use algorithms for closure properties to prove that this system is compatible with the functional equation for $a(x, 0, t)$. Like before, it then follows that the unique power series solution in $C(x)[[t]]$ of this functional equation is D-finite, and consequently, again using closure properties, the trivariate generating function

$$a(x, y, t) = \frac{1 - \frac{t}{x}a(0, y, t) - \frac{t}{y}a(x, 0, t)}{1 - t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)}$$

is D-finite as well. The computations needed for this variant of the proof are substantially cheaper.

There is yet another way to deduce from the original functional equation that $a(x, y, t)$ is D-finite. Multiply the functional equation by x and then replace x by $1/x$ to obtain

$$\tfrac{1}{x}a(\tfrac{1}{x}, y, t) = \tfrac{1}{x} + \tfrac{t}{x}\big(x + y + \tfrac{1}{x} + \tfrac{1}{y}\big)a(\tfrac{1}{x}, y, t) - ta(0, y, t) - \tfrac{t}{xy}a(\tfrac{1}{x}, 0, t).$$

By subtracting this equation from the x-fold of the original equation, we can eliminate the term $a(0, y, t)$. The resulting equation can be rewritten to

$$y\big(1-t\big(x+y+\tfrac{1}{x}+\tfrac{1}{y}\big)\big)\big(xa(x, y, t)-\tfrac{1}{x}a(\tfrac{1}{x}, y, t)\big)=xy-\tfrac{y}{x}-txa(x, 0, t)+\tfrac{t}{x}a(\tfrac{1}{x}, 0, t).$$

In this equation, replace y by $1/y$ to get another equation that can be used to eliminate the terms $a(x, 0, t)$ and $a(\frac{1}{x}, 0, t)$, which are independent of y. This gives

$$xy\, a(x, y, t) - \tfrac{y}{x}a(\tfrac{1}{x}, y, t) - \tfrac{x}{y}a(x, \tfrac{1}{y}, t) + \tfrac{1}{xy}a(\tfrac{1}{x}, \tfrac{1}{y}, t) = \frac{xy - \frac{y}{x} - \frac{x}{y} + \frac{1}{xy}}{1 - t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)}.$$

Now observe that the left hand side is an element of $C[x, \frac{1}{x}, y, \frac{1}{y}][[t]]$, i.e., a power series in t whose coefficients are Laurent polynomials in x and y. Observe further that the four series in the sum on the left hand side have disjoint support. More precisely, the series $xy\, a(x, y, t)$ only consists of terms $x^i y^j t^n$ with $i, j > 0$ while none of the other series contains any such terms. Therefore, if we apply the C-linear operator $[x^> y^>]\colon C[x, \frac{1}{x}, y, \frac{1}{y}][[t]] \to C[x, y][[t]]$ that is defined by mapping all terms $x^i y^j t^n$ with $i < 0$ or $j < 0$ to zero and all other terms to themselves, we find

$$xy\, a(x, y, t) = [x^> y^>]\frac{xy - \frac{y}{x} - \frac{x}{y} + \frac{1}{xy}}{1 - t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)},$$

and thus

$$a(t) = \left([x^> y^>]\frac{xy - \frac{y}{x} - \frac{x}{y} + \frac{1}{xy}}{1 - t\big(x + y + \frac{1}{x} + \frac{1}{y}\big)}\right)_{x=y=1}.$$

As the rational function $\frac{yx-\frac{y}{x}-\frac{x}{y}+\frac{1}{xy}}{1-t\left(x+y+\frac{1}{x}+\frac{1}{y}\right)}$ is clearly D-finite and the class of D-finite functions is closed under taking positive parts and evaluation (Sect. 5.3), it follows again that $a(t)$ is D-finite. Moreover, we can explicitly construct an annihilating operator for $a(t)$ from the above formula using creative telescoping (Chap. 5).

It is interesting to see what happens if we change the lattice walk model slightly. We continue to consider lattice walks in $\mathbb{N}^2$ starting at the origin and consisting of n steps, but instead of the set $\{\uparrow, \downarrow, \leftarrow, \rightarrow\}$ of admissible steps, we consider other subsets of $\{\uparrow, \downarrow, \leftarrow, \rightarrow, \searrow, \swarrow, \nwarrow, \nearrow\}$. For some subsets, we can proceed exactly as above and obtain a D-finite generating function. In some cases the generating function is even algebraic (e.g., for $\{\leftarrow, \downarrow, \nearrow\}$). On the other hand, there are also some step sets for which the generating function is not D-finite. Among those, there are some whose generating function is differentially algebraic (e.g., $\{\leftarrow, \uparrow, \rightarrow, \swarrow\}$) and some for which not even such a nonlinear differential equation exists (e.g., $\{\leftarrow, \uparrow, \downarrow, \nearrow\}$). The full story can be found in [57, 74, 105, 173, 192] and the references provided there.

Lattice walks play an important role in combinatorics because counting problems for many other combinatorial objects can be translated into counting problems for certain kinds of lattice walks. But within the area of combinatorics, D-finite functions appear not only in relation to restricted lattice walks. For example, D-finite functions are also encountered in counting permutations [72], integer points in polytopes [46], rhombus tilings [176], or various kinds of graphs [340]. D-finite functions can also be found outside of combinatorics, primarily in the following four areas that are strongly related to each other and to combinatorics. Here we only make some sketchy remarks intended for merely getting a rough impression, and we give some example references.

- Particular functions that arise often enough in applications that it makes sense to give them a name are called *special functions.* Typical examples are the trigonometric functions or the error function. Because of the importance of these functions, they are systematically investigated, and the collected knowledge about them is made available in textbooks [32, 364] and tables [27, 337]. Many classical special functions are D-finite, and for these functions, it is possible to generate collections of formulas automatically. An implementation of this idea is the Dynamic Dictionary of Mathematical Functions (DDMF) by Benoit, Chyzak, Darrasse, Gerhold, Mezzarobba, and Salvy [53].
- Many D-finite special functions originate from *physics*. For example, Bessel functions are used for describing the vibration of membranes, Airy functions appear in optics, and the analysis of a harmonic oscillator leads to Hermite polynomials. Physics also gives rise to many D-finite functions that have not (yet) acquired special names. For example, Feynman integrals, which are used to describe interactions between elementary particles, fall into the category of D-finite objects. See the volume of Schneider and Blümlein [397] for an overview of applications of computer algebra to particle physics. Another part of physics in which nameless D-finite functions arise naturally is statistical mechanics [85, 103, 104].
- D-finite functions are also used in *number theory.* For example, Apéry's proof of the irrationality of $\zeta(3)$ relies on computing recurrence equations satisfied by cer-

tain sums (cf. Exercise 17 in Sect. 5.4). In fact, van der Poorten's exposition [439] of Apéry's proof contains the first mention of "creative telescoping", the subject of Chap. 5. Zeilberger and Zudilin obtained irrationality proofs of various other constants by automatizing Apéry's proof [472]. Besides its relevance for proving that $\zeta(3) \notin \mathbb{Q}$, Apéry's sum and similar D-finite sequences enjoy interesting congruence relations [63, 417, 418]. Chen, Hou and Zeilberger [142] and Hou and Liu [240] discuss how such congruences can be discovered and proved automatically.
- In computer science, D-finite functions arise in the *analysis of algorithms*. Knuth's classical text on The Art of Computer Programming is full of examples of D-finite sequences, especially volume 3 on sorting and searching [281]. Techniques for analyzing the average case complexity of algorithms are provided by analytic combinatorics, an area shaped by Flajolet and Sedgewick [195]. D-finite power series are obtained naturally in applications of their "symbolic method" that systematically translates recursive specifications into generating functions. Moreover, D-finiteness finds applications in *program verification*. Kovács and her collaborators use recurrences to automatically identify loop invariants [243, 296, 297].

In addition to these rather established application areas in which D-finite functions and the corresponding computer algebra tools are meanwhile used routinely, D-finite functions are sometimes also found in more exotic contexts. Here are some examples.

- In *numerical engineering,* especially in the method of finite elements, bases of orthogonal polynomials are used to ensure sparsity of huge linear systems. Classical families of orthogonal polynomials are sufficient for most classical applications of the method, but there are also applications for which specialized basis functions need to be designed. The methodology of D-finiteness supports such designs, as shown for example by Pillwein [357] and Beuchler, Pillwein, and Zaglmayr [61, 62].
- In *knot theory,* it can be difficult to recognize whether two given knots are equal. A common approach is to evaluate certain invariants and to observe that knots for which an invariant evaluates to different values cannot be equal. A powerful invariant is the so-called colored Jones function, a quantity that is D-finite with respect to the q-shift. Garoufalidis and Koutschan compute a minimal annihilating operator for several specific knots [201, 203].
- In *chemistry,* benzenoid hydrocarbons are molecules whose structure amounts to a finite connected region without holes in a hexagonal lattice. The question is how many such molecules can be formed from n hexagons. The exact answer is only known for $n \leq 35$, and the counting sequence does not seem to be D-finite, but approximations by D-finite functions allow accurate and efficient estimates of the number of structures for moderate sizes of n, cf. the paper of Vöge, Guttmann, and Jensen [451].
- In *computational algebra,* it has been suggested by Cormier, Singer, and Ulmer [165] to exploit the D-finiteness of algebraic functions (Theorem 3.29)

for accelerating the computation of Galois groups of a polynomial $f \in \bar{\mathbb{Q}}(x)[y]$. The advantage of their approach is that the differential equation satisfied by an algebraic function is often considerably smaller than the minimal polynomial. Bostan, Gaudry, and Schost [82] used efficient evaluation of D-finite sequences to speed up integer factorization.

- In *biology,* the Canham model explains the shapes of membranes. Yu and Chen [465] showed that the model admits a unique solution of genus 1 provided that all the terms of a certain D-finite sequence $(u_n)_{n=0}^{\infty}$ in $\mathbb{Q}^{\mathbb{N}}$ are positive. The required positivity result was proven by Melczer and Mezzarobba [322] and again by Bostan and Yurkevich [78]. Dong, Melczer and Mezzarobba turned the proof technique of the first proof into a general algorithm that finds asymptotic expansions of D-finite sequence with certified explicit error bounds [172].
- In *coding theory,* one is interested in k-dimensional subspaces U of n-dimensional $\mathbb{F}$-vector spaces V such that $U \setminus \{0\}$ contains only vectors with at least d nonzero components, for a finite field $\mathbb{F}$ and certain numbers n, k, d such that $d + k - n$ is large. As noticed by Boucher, Geiselmann, and Ulmer [99–101], good settings can be achieved with ambient spaces V of the form $\mathbb{F}[\partial]/\langle L\rangle$, where $\mathbb{F}[\partial]$ is an Ore algebra (cf. Chap. 4) and $\langle L\rangle$ a suitably chosen left ideal.
- In *control theory,* the state of a system, expressed as a vector-valued function, and the control parameters, also expressed as a vector-valued function, are related through a system of linear differential equations. One of the questions is whether the state of the system can be influenced via the control parameters. Such questions can be answered algorithmically by studying properties of the Ore algebra module describing the differential equations, as explained, e.g., in a survey of Robertz [372].
- In *cryptography,* the Diffie-Hellman protocol is a way to generate shared secrets between parties connected by an insecure channel. Originally based on the group $(\mathbb{Z}_p \setminus \{0\}, \cdot)$, the idea of the protocol works for many other algebraic structures. Burger and Heinle [119] propose a version based on multivariate Ore algebras, arguing that the difficulty of factorization in these non-commutative rings ensures the security of this choice. The use of univariate Ore algebras had been suggested before [102] but this first idea was recognized as insecure [178].
- In *statistics,* the maximum likelihood estimation finds the parameters of a statistical model that best fits the observed data. This estimation requires the minimization of a multivariate function describing the probability distribution of the assumed statistical model. This function often is D-finite, and in this case, the minimization problem can be solved by the so-called holonomic gradient method proposed by Nakayama, Nishiyama, Noro, Ohara, Sei, Takayama, and Takemura [334].
- In *spaceflight,* uncontrolled debris forms a severe hazard to satellites and space stations. The positions and velocities of pieces of debris are permanently observed from earth, and this data is used to generate warnings about pieces with trajectories that might cause undesired collisions. Serra, Arzelier, Joldes,

Lasserre, Rondepierre, and Salvy managed to increase the accuracy of such collision forecasts significantly by using a custom-tailored D-finite function [402].

- In *sociology,* Schelling's models of segregation are finite dynamical systems that can indicate an inherent tendency of populations to develop clusters of members belonging to the same group. In an attempt to turn this qualitative observation into a quantitative result, Gerhold, Gebsky, Schneider, Weiss, and Zimmermann [211] define a notion of entropy for measuring how segregated a system is. For one-dimensional lattices (i.e., chains and circles), they show that the entropy is a D-finite function, and determine its asymptotics.
- In *simulation,* Quasi-Monte Carlo methods estimate high dimensional integrals by evaluating the integrand on sets of sample points chosen by a carefully designed pseudo-random number generator. The goal is to get sets of sample points for which the variance of the resulting estimate for the integral is small. Wiart and Wong [455] observe that for a popular pseudo-random number generator used in this context, this analysis leads to questions that can be addressed by algorithms for D-finite functions.

1.4 Computer Algebra

Algorithms for D-finite functions rely heavily on techniques from computer algebra which are interesting in their own right and useful in many other contexts. In the present section we give a quick summary of some fundamental facts from computer algebra which we shall take for granted later. Readers who are not familiar with this material and would like to know more about it are referred to specialized textbooks on the subject. Some references are given at the end of this section.

Every integer can be represented by a sign and a finite list of digits in some fixed base. Let us make the convention that the base is 2. We then also say *bit* instead of digit. Arithmetic can be performed with bit representations. For example, there is an algorithm which for any two given integers computes their sum. More precisely, the algorithm takes the bit representations of two integers as input and returns a bit representation of their sum as output. The algorithm may proceed bit by bit, like in the usual hand calculation, and the number of bit operations it has to perform in total can be taken as a measure of the computation time. In the case of addition, this number is proportional to the number of bits in the input.

Addition is simple enough that we could work out the number of required bit operations explicitly. This number, depending on the input size, is called the *complexity* of the algorithm. For more sophisticated operations, it is often not possible to determine the complexity explicitly. The exact number of operations is also not too important. What we really want to know is how fast the computation time grows when the input size increases. Complexity estimates are therefore commonly stated in terms of asymptotic estimates. For two functions $f, g\colon \mathbb{N} \to \mathbb{R}$, we write $f(n) = \mathrm{O}(g(n))$ if there exist $c > 0$ and $n_0 \in \mathbb{N}$ such that $|f(n)| < cg(n)$

for all $n \geq n_0$. For example, we would say that adding two integers with n bits costs $\mathrm{O}(n)$ bit operations.

One feature of the O-notation is that it focuses on the behaviour for large n. Another feature is that it expresses only an upper bound, so if one algorithm has complexity $\mathrm{O}(n^2)$ and another has complexity $\mathrm{O}(n^3)$, we cannot conclude that the first is faster, because the actual complexities may have been $n^2 = \mathrm{O}(n^2)$ and $n = \mathrm{O}(n^3)$, respectively. A third feature is that it suppresses multiplicative constants, e.g., if we have $f(n) = \mathrm{O}(5n)$ then we also have $f(n) = \mathrm{O}(10^{-5}n)$. While multiplicative constants do affect the actual performance of an algorithm, it is a convenient simplification to ignore them in the analysis. In fact, it is sometimes appropriate to drop not only multiplicative constants, but also logarithmic terms. The *soft-O notation* $f(n) = \mathrm{O}^{\sim}(g(n))$ means that there exists a $k \in \mathbb{N}$ such that $f(n) = \mathrm{O}(g(n)(\log g(n))^k)$.

The classical algorithm for multiplying two integers needs $\mathrm{O}(n^2)$ bit operations to multiply two integers with n bits. It turns out that with more sophisticated algorithms a better complexity bound can be achieved. Algorithms commonly used in computer algebra software need only $\mathrm{O}(n \log(n) \log\log(n)) = \mathrm{O}^{\sim}(n)$ bit operations for multiplying two integers of length n. In theory, the bound can be reduced even further, but it is not known to which limit. Instead of making a particular assumption about the cost for multiplying integers, we therefore introduce a place holder for this complexity.

Definition 1.15 A function $\mathrm{M}_{\mathbb{Z}} : \mathbb{R} \to \mathbb{R}$ is called an *integer multiplication time* if there exists an algorithm which for any two integers with at most n bits can compute their product using no more than $\mathrm{M}_{\mathbb{Z}}(n)$ bit operations. □

Once and for all, fix such a function $\mathrm{M}_{\mathbb{Z}}$. We will express complexity estimates of algorithms that involve integer multiplication in terms of this function. At any time, we may replace $\mathrm{M}_{\mathbb{Z}}(n)$ by $\mathrm{O}(n \log(n) \log\log(n))$ or better bounds. It is fair to assume that $\mathrm{M}_{\mathbb{Z}}(n)$ grows at least linearly and at most quadratically, so we may assume that $\mathrm{M}_{\mathbb{Z}}(n)/n \geq \mathrm{M}_{\mathbb{Z}}(m)/m > 0$ for all $n \geq m > 0$ and that $\mathrm{M}_{\mathbb{Z}}(mn) \leq m^2 \mathrm{M}_{\mathbb{Z}}(n)$ for all $n, m \geq 0$.

The following theorem is a collection of other important integer operations and their corresponding costs. Note that while some of the operations are rather simple, the claimed complexity bounds are not at all obvious.

Theorem 1.16

1. *(Division with remainder) There is an algorithm which for any two integers $a, b \in \mathbb{Z}$, $b \neq 0$ with at most n bits computes integers $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < |b|$, and which uses at most $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(n))$ bit operations.*
2. *(Greatest common divisor; extended Euclidean algorithm) There is an algorithm which for any two integers $a, b \in \mathbb{Z}$ with at most n bits computes their greatest common divisor $g \in \mathbb{Z}$ as well as $p, q \in \mathbb{Z}$ with $g = ap + bq$, and which uses at most $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(n) \log(n))$ bit operations.*
3. *(Simultaneous modular reduction) There is an algorithm which for any given $m_1, \ldots, m_k \in \mathbb{N} \setminus \{0, 1\}$ and any $a \in \mathbb{Z}$ with $|a| < m := \prod_{i=1}^{k} m_i$ can compute*

$a \bmod m_1, \ldots, a \bmod m_k$, and which uses at most $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(\log(m)) \log\log(m))$ *bit operations.*

4. *(Chinese remainder theorem) There is an algorithm which for any $m_1, \ldots, m_k \in \mathbb{N} \setminus \{0, 1\}$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and any $r_1, \ldots, r_k \in \mathbb{N}$ with $r_i < m_i$ for $i = 1, \ldots, k$ computes the unique $a \in \{0, \ldots, m-1\}$ with $m = \prod_{i=1}^k m_i$ such that $a \equiv r_i \bmod m_i$, and which uses at most* $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(\log(m)) \log\log(m))$ *bit operations.*
5. *(Rational reconstruction) There is an algorithm which for any $m, k, a \in \mathbb{N} \setminus \{0\}$ with $a, k \leq m$ computes $p, q \in \mathbb{Z}$ such that $p \equiv aq \bmod m$ and $|p| < k$ and $0 \leq q \leq m/k$, and which uses at most* $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(\log(m)) \log\log(m))$ *bit operations.* □

Proof 1. is Thm. 1.4 of [109] and Thm. 9.8 of [204]; 2. is Thm. 4.2 of [452]; 3. and 4. are in Sect. 2.7 of [109], and they also appear as Thms. 10.24 and 10.25 in [204]; 5. is Thm. 5.26 in [204] in combination with part 2. ■

In the notation of part 1, we call q the *quotient* and r the *remainder* of the division of a by b and write $q = \mathrm{quo}_{\mathbb{Z}}(a, b)$ and $r = \mathrm{rem}_{\mathbb{Z}}(a, b)$. In the case $r = 0$ we say that b *divides* a, that b is a *divisor* of a, or that a is a *multiple* of b (in $\mathbb{Z}$). In this case we write $b \mid a$. We write $\gcd_{\mathbb{Z}}(a, b)$ for the greatest common divisor of the integers $a, b \in \mathbb{Z}$: it is defined as the largest nonnegative integer which is a divisor of both a and b. The numbers $p, q \in \mathbb{Z}$ of part 2 are called *cofactors* of a and b. The numbers a, b are called *coprime* if $\gcd_{\mathbb{Z}}(a, b) = 1$.

Using the operations of Theorem 1.16, we can not only compute with integers but also with rational numbers. A rational number $\frac{p}{q}$ is a pair (p, q) of integers with $q \neq 0$. If p and q have common factors, we can *cancel* them, in particular we have $\frac{p}{q} = \frac{\mathrm{quo}_{\mathbb{Z}}(p, \gcd_{\mathbb{Z}}(p,q))}{\mathrm{quo}_{\mathbb{Z}}(q, \gcd_{\mathbb{Z}}(p,q))}$ and may thus assume that the numerator and denominator are coprime. By multiplying the numerator and denominator by -1 if necessary, we can furthermore assume that the denominator is positive.

The operations of Theorem 1.16 also support computations in *residue class rings*. For a fixed $m \in \mathbb{N} \setminus \{0, 1\}$, two integers $a, b \in \mathbb{Z}$ are called *equivalent modulo m* if $m \mid a - b$. This equivalence is an equivalence relation, and the set of equivalence classes, denoted by $\mathbb{Z}_m$, becomes a ring if we define $[a] + [b] := [a + b]$ and $[a][b] := [ab]$. Since we have $[a] = [\mathrm{rem}(a, m)]$ for all $a \in \mathbb{Z}$, every equivalence class contains exactly one element of $\{0, 1, \ldots, m-1\}$, which can be used to represent the class. In particular, we have $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. The notation $a \equiv b \bmod m$ already used in Theorem 1.16 means that $[a] = [b]$ as elements of $\mathbb{Z}_m$.

If m is a prime, then $\mathbb{Z}_m$ is a field. To see this, note that $[a] = [0]$ iff $m \mid a$, so for every class $[a] \in \mathbb{Z}_m \setminus \{[0]\}$ we have $m \nmid a$, which implies $\gcd_{\mathbb{Z}}(m, a) \neq m$. Since the gcd must be a divisor of m and m is a prime, the only remaining possibility is $\gcd_{\mathbb{Z}}(m, a) = 1$. But then, in view of part 2 of Theorem 1.16 we have cofactors $p, q \in \mathbb{Z}$ with $1 = mp + aq$, which means $[1] = [a][q]$, so $[q]$ is a multiplicative inverse of $[a]$. We see that if m is prime, a multiplicative inverse exists for every nonzero element of $\mathbb{Z}_m$, and its computation costs $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(m) \log(m))$ bit operations.

Parts 3 and 4 of Theorem 1.16 provide operations for translating a computation in $\mathbb{Z}$ into several computations in residue class rings $\mathbb{Z}_m$ and back. The operation in part 3 amounts to a ring homomorphism $\mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. Instead of computing with integers in order to solve a certain problem, we compute with the corresponding *homomorphic images,* which, depending on the problem at hand, may be more efficient. The operation in part 4 lets us translate a homomorphic image back to an integer. More precisely, it provides a ring homomorphism from $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ to $\mathbb{Z}_{m_1 \cdots m_k}$ whenever the m_i are pairwise coprime. If the product $m_1 \cdots m_k$ is sufficiently large, the integer answer to the original problem can be extracted from its image in $\mathbb{Z}_{m_1 \cdots m_k}$.

Example 1.17 For the matrix

$$A = \begin{pmatrix} 6270 & 87412 & 62574 & -96343 \\ 26869 & 92356 & -99752 & -76532 \\ -60746 & 46114 & -74307 & 79100 \\ -75163 & 28921 & -11365 & -21420 \end{pmatrix} \in \mathbb{Z}^{4\times 4},$$

we have $\det(A) = -1274054553596291 58201$. Instead of computing the determinant directly with integer arithmetic, we can view the matrix entries as elements of $\mathbb{Z}_m$, for various choices of m, and compute the determinant there.

Viewing the entries of A as elements of $\mathbb{Z}_{1009}$, we can simplify the matrix to

$$\begin{pmatrix} 216 & 638 & 16 & 521 \\ 635 & 537 & 139 & 152 \\ 803 & 709 & 359 & 398 \\ 512 & 669 & 743 & 778 \end{pmatrix}.$$

The determinant of this matrix, viewed as an element of $\mathbb{Z}_{1009}$, is 8. This implies that in $\mathbb{Z}$ we have $\det(A) = 1009q + 8$ for some $q \in \mathbb{Z}$.

Part 3 allows us to perform the simplification above efficiently not only for a single m but for several of them, say for the first ten primes above 1000. For these matrices, we then compute the determinant in the respective residue class ring $\mathbb{Z}_m$. The result is as follows:

m	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061
$\operatorname{rem}(\det(A), m)$	8	966	871	115	147	687	792	860	421	545

Given this data, the algorithm behind part 4 of Theorem 1.16 finds that

$$\begin{aligned} &\operatorname{rem}(\det(A), 1376476052812256418701683532789) \\ &= 1376476052684850963342054374588. \end{aligned}$$

Note that 1376476052812256418701683532789 is the product of the primes in the first row of the table above. Like before, the result means that in $\mathbb{Z}$ we have

$$\det(A) = 1376476052812256418701683532789q \\ + 1376476052684850963342054374588$$

for some $q \in \mathbb{Z}$. The choices $q = -2, -1, 0, 1, 2$ correspond to the candidates

$$-1376476052939661874061312690990,\\ -127405455359629158201,\\ 1376476052684850963342054374588,\\ 2752952105497107382043737907377,\\ 4129428158309363800745421440166.$$

The theorem does not tell us which choice of q is right, but we can be sure that if the product $m_1 \cdots m_k$ is sufficiently large, then the right answer is the candidate with minimal absolute value. More precisely, if we know for other reasons that the answer to the integer problem is bounded in absolute value by M, then it suffices to ensure that $m_1 \cdots m_k$ exceeds $2M$, and the integer answer is either the output a of the algorithm from part 4 or $a - m_1 \cdots m_k$, depending on which of these two numbers has smaller absolute value. In the present example, if we know for some reason that $|\det(A)| < 10^{25}$, this bound together with the calculation documented above implies $\det(A) = -127405455359629158201$. □

Part 5 of Theorem 1.16 is useful when the original problem is not about integers but about rational numbers. In this case, we can still translate the problem into finite domains $\mathbb{Z}_m$, as long as the moduli m are chosen such that they are coprime with all of the denominators that would arise if the problem were solved by computing in $\mathbb{Q}$. Typically, this condition is not easy to ensure a priori, but fortunately, it usually suffices in practice to choose reasonably large moduli. Moduli not satisfying the condition might lead to wrong output. These are called *unlucky,* and although there is usually no way to tell what they are in advance, in many applications we can easily recognize them at the end of a computation. If we encounter one, we simply discard the result and try another. Once we know the homomorphic image of the result with respect to a sufficiently large modulus, the algorithm behind part 5 of Theorem 1.16 allows us to translate it back into a rational number.

Example 1.18 For the matrix

$$A = \begin{pmatrix} 11/29 & 3/13 & 2/11 & 11/31 \\ 23/3 & 19/23 & 5/2 & 17/31 \\ 19/3 & 13/19 & 17/2 & 31/2 \\ 31/11 & 1 & 13/17 & 3/7 \end{pmatrix} \in \mathbb{Q}^{4\times 4},$$

we have $\det(A) = \frac{6126061079}{5656834337}$. Instead of computing the determinant directly in $\mathbb{Q}$, we can view the matrix entries as elements of $\mathbb{Z}_m$, for various choices of m, and compute the determinant there. For example, the matrix entry $\frac{11}{29}$ corresponds to the element 905 of $\mathbb{Z}_{1009}$ because $11 \equiv 905 \cdot 29 \bmod 1009$. This can be found using part 2 of Theorem 1.16.

When we compute the determinant of A in $\mathbb{Z}_m$ for m running through the first ten primes above 1000 and then use part 4 to merge these homomorphic images into one, we obtain the result 250701197724587302257631313694. Using rational reconstruction, we can find rational numbers u/v that correspond to this number in $\mathbb{Z}_{1376476052812256418701683532789}$. There are many such numbers, and the algorithm behind part 5 of the theorem allows us to specify in some sense how the information encoded in the homomorphic image should be divided into a numerator and a denominator. Here are some of the possible outcomes:

k	numerator	denominator
10^6	-231383	997182470694199551726209
10^8	-11043235	1348151154611345663741
10^{10}	6126061079	5656834337
$\vdots$	$\vdots$	$\vdots$
10^{20}	6126061079	5656834337
10^{22}	8273211306456040551653	72107965
10^{24}	$-553575168299626899977626$	75747

Theorem 1.16 provides no clue which of these candidates, if any, is the right result. However, it can be further shown that for any prescribed k there is at most one reconstruction result whose numerator is bounded by $k/2$, i.e., the rational number associated to a fixed k is essentially unique. Therefore, if we happen to have a bound M on the numerator and the denominator of the rational answer, we can choose $k = 2M$ and a modulus larger than $2M^2$ in order to be sure to get the right result. In the present example, if we know for some reason that numerator and denominator of $\det(A)$ are bounded by 10^{12}, this information together with the calculation documented above implies $\det(A) = \frac{6126061079}{5656834337}$. □

Computing in homomorphic images can be viewed as a kind of approximation: by doing a computation modulo a prime with 64 bits, we roughly obtain information equivalent to 64 bits of the answer. It is also possible to do approximate computations in the usual sense.

Theorem 1.19 *Suppose that $z_1, z_2 \in \mathbb{R}$ are fixed numbers for which we know (or can determine) any number of digits in their binary (or decimal) expansion.*

1. *Computing n digits of the binary (or decimal) expansion of $z_1 + z_2$ from the known digits of z_1 and z_2 requires no more than $\mathrm{O}(n)$ bit operations.*
2. *Computing n digits of the binary (or decimal) expansion of $z_1 z_2$ from the known digits of z_1 and z_2 requires no more than $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(n))$ bit operations.*

3. *If $z_2 \neq 0$, computing n digits of the binary (or decimal) expansion of z_1/z_2 from the known digits of z_1 and z_2 requires no more than $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(n))$ bit operations* □

Proof 1. cf. Sect. 3.2 in [109]; 2. cf. Sect. 3.3 in [109]; 3. cf. Sect. 3.4 in [109]. ■

Let us now turn from numbers to polynomials. Recall from Sect. 1.1 that for a ring R, we write $R[x]$ for the ring of univariate polynomials with coefficients in R. The degree of a polynomial p is denoted by $\deg(p)$ or $\deg_x(p)$ and its *leading coefficient* by $\mathrm{lc}(p)$. We write $[x^n]p$ for the coefficient of x^n in p. For $n \notin \mathbb{N}$, we set $[x^n]p$ to zero. Note that $\mathrm{lc}(p) = [x^{\deg(p)}]p$. A polynomial is called *monic* if its leading coefficient is 1. In order to emphasize that $p, q, \ldots$ are polynomials in x, we sometimes also use the notation $p(x), q(x), \ldots$.

Polynomials can be represented in various ways. The most common ways are the *dense representation* and the *sparse representation.* In the dense representation, a polynomial is encoded as a list of coefficients. For example, $x^4 + 2x - 5$ is encoded as $(-5, 2, 0, 0, 1)$. The sparse representation of a polynomial consists of a set of pairs, each consisting of the coefficient and the exponent of a term, e.g., $\{(-5, 0), (2, 1), (1, 4)\}$. Techniques and complexity statements depend heavily on the underlying representation. In this text, unless otherwise stated, we assume that the dense representation is used.

The cost of polynomial arithmetic depends not only on the chosen representation, but also on the coefficient domain R. One way to deal with this issue is to measure the cost of an operation on polynomials in terms of the number of operations in R that an algorithm has to perform in order to carry out the operation. We call this the *arithmetic complexity* of the algorithm. Unless R is a finite domain, the arithmetic complexity does not adequately reflect the actual runtime of an algorithm, but it has the advantage that statements can be made independent of the choice of R. For example, adding two polynomials of degree at most n requires no more than $\mathrm{O}(n)$ operations in R. No statement is made on how costly these operations in R are.

Multiplication is more difficult. The classical algorithm needs $\mathrm{O}(n^2)$ operations in R to multiply two polynomials of degree $\leq n$, but more efficient algorithms are known. Most computer algebra systems nowadays use an algorithm which requires $\mathrm{O}(n \log(n) \log\log(n)) = \mathrm{O}^{\sim}(n)$ operations in R, a bound which at least in theory can still be improved. As before, instead of making a particular assumption on the multiplication cost, we introduce a place holder.

Definition 1.20 A function $\mathrm{M}\colon \mathbb{R} \to \mathbb{R}$ is called a *(polynomial) multiplication time* if for every ring R there exists an algorithm which for any two polynomials in $R[x]$ of degree at most n computes their product using no more than $\mathrm{M}(n)$ ring operations in R. □

Once and for all, fix such a function M. We will express complexity estimates of algorithms involving polynomial multiplication in terms of this function, keeping in mind that we may replace $\mathrm{M}(n)$ by $\mathrm{O}(n \log(n) \log\log(n))$ or better bounds, or by $\mathrm{O}^{\sim}(n)$. Polynomial multiplication is closely related to integer multiplication. In particular, we may again assume that $\mathrm{M}(n)/n \geq \mathrm{M}(m)/m > 0$ for all $n \geq m > 0$ and that $\mathrm{M}(mn) \leq m^2\mathrm{M}(n)$ for all $n, m \geq 0$.

We will make use of the following fundamental facts about computing with univariate polynomials with coefficients in a field C of characteristic zero. Note that most items have a counterpart for integers in Theorem 1.16.

Theorem 1.21

1. *(Division with remainder) There is an algorithm which for any two polynomials* $a, b \in C[x]$*,* $b \neq 0$ *of degree at most* n *computes polynomials* $q, r \in C[x]$ *with* $a = bq + r$ *and* $\deg(r) < \deg(b)$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n))$ *operations in* C*.*
2. *(Greatest common divisor; extended Euclidean algorithm) There is an algorithm which for any two polynomials* $a, b \in C[x]$ *of degree at most* n *computes their greatest common divisor* $g \in C[x]$ *as well as* $p, q \in C[x]$ *with* $g = ap + bq$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n)\log(n))$ *operations in* C*.*
3. *(Shift) There is an algorithm which for any polynomial* $p \in C[x]$ *of degree at most* n *and any* $c \in C$ *computes the coefficients of the polynomial* $p(x + c) \in C[x]$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n))$ *operations in* C*.*
4. *(Simultaneous evaluation) There is an algorithm which for any* $m_1, \ldots, m_k \in C[x]$ *of degree at least* 1 *and any* $a \in C[x]$ *with* $\deg(a) < n := \sum_{i=1}^{k} \deg(m_i)$ *can compute* $a \bmod m_1, \ldots, a \bmod m_k$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n)\log(n))$ *operations in* C*.*
5. *(Interpolation) There is an algorithm which for any* $m_1, \ldots, m_k \in C[x]$ *of degree at least* 1 *with* $\gcd(m_i, m_j) = 1$ *for* $i \neq j$ *and any* $r_1, \ldots, r_k \in C[x]$ *with* $\deg(r_i) < \deg(m_i)$ *for* $i = 1, \ldots, k$ *computes the unique* $a \in C[x]$ *of degree at most* $n := \sum_{i=1}^{k} \deg(m_i)$ *such that* $a \equiv r_i \bmod m_i$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n)\log(n))$ *operations in* C*.*
6. *(Rational reconstruction) There is an algorithm which for any* $m, a \in C[x] \setminus \{0\}$ *with* $\deg(a) < \deg(m)$ *and any* $k \in \mathbb{N}$ *with* $0 \leq k \leq n =: \deg(m)$ *computes* $p, q \in C[x]$ *such that* $p \equiv aq \bmod m$ *and* $\deg(p) < k$ *and* $\deg(q) \leq n - k$*, and which uses no more than* $\mathrm{O}(\mathrm{M}(n)\log(n))$ *operations in* C*.* □

Proof 1. is Thm. 9.6 in [204]; 2. is Cor. 11.9 in [204]; 3. is Thm. 9.15 in [204]; 4. is Cor. 10.17 in [204]; 5. is Cor. 10.23 in [204]; 6. is Thm. 5.16 in [204]. ■

The polynomials q and r of part 1 are called the *quotient* and *remainder,* respectively, of the division of a by b, and we use the notation $q = \mathrm{quo}(a, b)$ and $r = \mathrm{rem}(a, b)$ for them. If $\mathrm{rem}(a, b) = 0$, we say that b *divides* a and write $b \mid a$. Then b is called a *divisor* of a and a is called a *multiple* of b. The greatest common divisor of two polynomials a, b is defined as the unique monic polynomial g which is a divisor of a and b and a multiple of any other divisor of a and b. We denote the greatest common divisor of a, b by $g = \gcd(a, b)$. If there is a chance of confusion, we also use the notation $\gcd_x(a, b)$ to emphasize that a, b are understood as elements of $C[x]$. In the case $\gcd(a, b) = 1$, we say that a and b are *coprime.*

A rational function $r \in C(x)$ is a fraction with polynomials (i.e., elements of $C[x]$) as numerator and denominator. Using the Euclidean algorithm, we can find common factors in the numerator and the denominator of a given rational function, and using the division algorithm of part 1, we can cancel these common factors. Moreover, by dividing the numerator and the denominator by the leading coefficient of the denominator, we can always ensure that the polynomial in the denominator is monic. It is a good idea to invest the time it takes to keep rational functions canceled at all times, because if we don't do this, common factors accumulate and can quickly reach an unreasonable size that makes it impossible to complete a computation. Whether it is also a good idea to make the denominator monic depends on the coefficient field C. For example, for $C = \mathbb{Q}$ it may be better to store a rational function as a quotient of two polynomials with integer coefficients, i.e., elements of $\mathbb{Z}[x]$, and take care that not only common polynomial factors but also common integer factors are canceled. For example, we might want to store $\frac{5x-10}{15x+5}$ as $\frac{x-2}{3x+1}$ rather than as $\frac{x/3-2/3}{x+1/3}$.

Polynomial arithmetic also allows us to perform computations in algebraic extensions. Fix a polynomial $m \in C[x] \setminus C$ and call two polynomials $a, b \in C[x]$ equivalent if $m \mid a - b$. This is an equivalence relation on $C[x]$, and the set of equivalence classes, denoted by $C[x]/\langle m\rangle$, is a ring together with the operations $[a] + [b] := [a + b]$ and $[a][b] := [ab]$. In this construction the class $[x]$ is a root of the polynomial m. For example, in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ we have $[x]^2 - [2] = [x^2 - 2] = [0]$. Since for every $a \in C[x]$ we have $[a] = [\mathrm{rem}(a, m)]$, we can represent every element of $C[x]/\langle m\rangle$ as a polynomial of degree less than $\deg(m)$. This representation is unique. In fact, $C[x]/\langle m\rangle$ is a vector space over C, and $\{[1], [x], \ldots, [x^{\deg(m)-1}]\}$ is a basis of this space.

A polynomial $m \in C[x] \setminus C$ is called *irreducible* if for any two polynomials $u, v \in C[x]$ with $m = uv$ we have $u \in C$ or $v \in C$. It turns out that the ring $C[x]/\langle m\rangle$ is a field if and only if m is irreducible. For, if $a \in C[x]$ is such that $[a] \neq [0]$, which means $m \nmid a$, then $\gcd(m, a) = 1$, because m is irreducible, and then, according to part 2 of Theorem 1.21, there are $p, q \in C[x]$ such that $1 = mp + aq$, which means $[1] = [a][q]$, so $[q]$ is a multiplicative inverse of $[a]$. If $n = \deg(m)$, then computing a multiplicative inverse costs $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations in C, addition costs $\mathrm{O}(n)$ operations, and multiplication costs $\mathrm{O}(\mathrm{M}(n))$ operations.

Example 1.22 Consider the field $C = \mathbb{Q}[x]/\langle x^2 - 2\rangle$. We use the symbol $\sqrt{2}$ to denote the equivalence class $[x]$ and write r instead of $[r]$ for every $r \in \mathbb{Q}$. With this notational convention, we can regard C as the smallest field containing $\mathbb{Q}$ and $\sqrt{2}$. We also use the notation $\mathbb{Q}(\sqrt{2})$ to denote this field. All of its elements can be written in the form $a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. For example

$$\frac{\frac{451}{131} - \frac{523}{813}\sqrt{2}}{\frac{325}{521} + \frac{392}{323}\sqrt{2}} + \frac{\frac{541}{113} - \frac{235}{231}\sqrt{2}}{\frac{352}{251} + \frac{932}{233}\sqrt{2}}$$
$$= \Big(-\frac{11186703711291331}{7710994955956569} + \frac{13812074599495453}{7710994955956569}\sqrt{2}\Big) + \Big(-\frac{3053171279}{6173777148} + \frac{769076801}{1122504936}\sqrt{2}\Big)$$

$$= -\frac{1028968934069529726005397 1}{528955160526977024140946 8} + \frac{2381607694176453675945753}{9617366555035945893471 76}\sqrt{2}.$$

It is typical for computations involving rational numbers that the numbers in the output have more digits than the numbers in the input. Note that in the arithmetic complexity we only count operations in C, which is equivalent to assuming that all operations in C take the same fixed (but positive) amount of time. □

Parts 4 and 5 of Theorem 1.21 allow us to translate a computational problem in $C[x]$ to several problems in C and to translate their solutions back to a solution of the original problem. For $p \in C[x]$ and $c \in C$ we have that $\mathrm{rem}(p, x - c)$ is a polynomial of degree less than 1, i.e., an element of C. This constant is typically denoted by $p(c)$ and it is called the *evaluation* of p at c. According to part 1 of the theorem, evaluating a polynomial of degree n at some field element costs not more than $\mathrm{O}(\mathrm{M}(n))$ operations in C. In fact, $\mathrm{O}(n)$ operations suffice (Exercise 15). According to part 4, the values of a polynomial p at several field elements can be obtained more efficiently than computing the evaluations separately. Part 5 allows us to go in the opposite direction, i.e., to compute a polynomial p which at prescribed field elements $c_1, \ldots, c_k$ has prescribed evaluations $p(c_1), \ldots, p(c_k)$. This process is called *interpolation*.

Example 1.23 For the matrix

$$A = \begin{pmatrix} 3x+2 & 3x & 3x+4 \\ 4x & 2x+3 & 3 \\ 2x+3 & 2 & 3 \end{pmatrix} \in \mathbb{Q}[x]^{3\times 3},$$

we have $\det(A) = -12x^3 - 28x^2 + 5x - 30$. Instead of computing the determinant directly, we can use part 4 to evaluate the entries of A at various rational numbers, say at $2, 3, 4, 5$, and then compute the determinants of the resulting matrices in $\mathbb{Q}^{3\times 3}$:

$$\det\begin{pmatrix} 8 & 6 & 10 \\ 8 & 7 & 3 \\ 7 & 2 & 3 \end{pmatrix} = -228, \qquad \det\begin{pmatrix} 11 & 9 & 13 \\ 12 & 9 & 3 \\ 9 & 2 & 3 \end{pmatrix} = -591,$$

$$\det\begin{pmatrix} 14 & 12 & 16 \\ 16 & 11 & 3 \\ 11 & 2 & 3 \end{pmatrix} = -1226, \quad \det\begin{pmatrix} 17 & 15 & 19 \\ 20 & 13 & 3 \\ 13 & 2 & 3 \end{pmatrix} = -2205.$$

Using part 5 to find a polynomial p with $p(2) = -228$, $p(3) = -591$, $p(4) = -1226$, $p(5) = -2205$ we obtain $p = -12x^3 - 28x^2 + 5x - 30$. This implies that there is a polynomial q such that

$$\det(A) = -12x^3 - 28x^2 + 5x - 30 + (x-2)(x-3)(x-4)(x-5)q.$$

Since the determinant can only be a polynomial of degree at most 3, the only possibility is $q = 0$. □

In combination with part 6, the technique of evaluation and interpolation can also be used in the context of rational functions, quite similar to how it was illustrated in Example 1.18 for rational numbers.

Polynomial arithmetic can also be used for computing with formal power series. Fix a positive integer N and consider two power series a, b as equivalent if the coefficients of x^i in $a - b$ is zero for $i = 0, \dots, N-1$. This is an equivalence relation on $C[[x]]$. The equivalence classes are called *truncated power series* and can be viewed as approximations of power series with accuracy N. The set of all truncated formal power series for a fixed N forms a ring which is isomorphic to $C[x]/\langle x^N \rangle$. For a power series with accuracy N we use the notation

$$a_0 + a_1 x + \cdots + a_{N-1} x^{N-1} + \mathrm{O}(x^N),$$

where the expression $\mathrm{O}(x^N)$ only indicates the accuracy and is not to be confused with the notation used for stating complexity estimates.

Theorem 1.24

1. *There is an algorithm which computes the first n terms of $a + b$ given the first n terms of $a, b \in C[[x]]$, and which uses no more than $\mathrm{O}(n)$ operations in C.*
2. *There is an algorithm which computes the first n terms of ab given the first n terms of $a, b \in C[[x]]$, and which uses no more than $\mathrm{O}(\mathrm{M}(n))$ operations in C.*
3. *There is an algorithm which computes the first n terms of the multiplicative inverse $1/a$ given the first n terms of $a \in C[[x]]$ with $a(0) \neq 0$, and which uses no more than $\mathrm{O}(\mathrm{M}(n))$ operations in C.*
4. *There is an algorithm which computes the first n terms of the composition $a \circ b$ from the first n terms of $a, b \in C[[x]]$ with $b(0) = 0$, and which uses no more than $\mathrm{O}(\sqrt{n \log(n)}\mathrm{M}(n))$ operations in C.*
5. *There is an algorithm which computes the first n terms of the compositional inverse a^{-1} given the first n terms of $a \in C[[x]]$ with $a(0) = 0$, and which uses no more than $\mathrm{O}(\sqrt{n \log(n)}\mathrm{M}(n))$ operations in C.* □

Proof 1. and 2. are obvious; 3. is Thm. 9.25 in [204]; 4. is Thm. 2.2 in [108]; 5. is Thm. 4.1 in [108]. ■

A polynomial $p \in C[x]$ is called *squarefree* if there does not exist a polynomial $q \in C[x] \setminus C$ with $q^2 \mid p$. Since C has characteristic zero, this is the case if and only if p and its derivative p' are coprime (Exercise 16).

Since we have $\deg(q^n) = n \deg(q) \geq n$ for every polynomial $q \in C[x] \setminus C$, there exists a largest $n \in \mathbb{N}$ with $q^n \mid p$. This integer is called the *valuation* or the *multiplicity* of p at q and denoted by $\nu_q(p)$. For a rational function $u/v \in C(x)$ with $u, v \in C[x]$, we define $\nu_q(u/v) := \nu_q(u) - \nu_q(v)$. If $\deg(q) = 1$ and $\xi \in C$ is the unique root of q, then we also write ν_ξ instead of ν_q.

For any polynomial p there are monic irreducible polynomials $p_1, \dots, p_n \in C[x]$ and $e_1, \dots, e_n \in \mathbb{N} \setminus \{0\}$ such that $p = \operatorname{lc}(p) p_1^{e_1} \cdots p_n^{e_n}$. These polynomials p_i are uniquely determined by p and are called its *irreducible factors*. Note that $\nu_{p_i}(p) = e_i$ for all i. The following theorem is a collection of some facts about polynomial factorization. The complexity estimates mentioned in parts 2–5 refer to randomized algorithms.

Theorem 1.25

1. *(squarefree decomposition) There is an algorithm which for a given polynomial $p \in C[x]$ of degree at most n computes its squarefree decomposition, i.e., monic squarefree and pairwise coprime polynomials $p_1, \dots, p_d$ such that $p = \operatorname{lc}(p) p_1 p_2^2 \cdots p_d^d$ and requires no more than $\mathrm{O}(\mathrm{M}(n) \log(n))$ operations in C.*
2. *There is an algorithm which for a given polynomial $p \in \mathbb{Z}_k[x]$ (k a prime with at most m bits) of degree at most n finds all of its irreducible factors and requires no more than $\mathrm{O}((\mathrm{M}(n^2) + m\mathrm{M}(n)) \log(n))$ bit operations.*
3. *There is an algorithm which for a given polynomial $p \in \mathbb{Q}[x]$ of degree at most n and coefficients with at most m bits finds all of its irreducible factors and requires no more than $\mathrm{O}^\sim(n^8(n^2 + m^2))$ bit operations.*
4. *If C is such that there is a factorization algorithm for polynomials in $C[x]$, then there are also factorization algorithms for $C[x_1, \dots, x_n]$ and for $C(\alpha)[x]$, where $C(\alpha)$ is an algebraic extension field of C.*
5. *There is an algorithm which for a given polynomial $p \in \mathbb{Z}[x]$ of degree at most n and coefficients with at most m bits finds all of the integer roots of p and needs no more than $\mathrm{O}(\mathrm{M}(n) \log(n)(m + \log(n))\mathrm{M}(m + \log(n)) \log(m + \log(n))) = \mathrm{O}^\sim(nm^2)$ bit operations.* □

Proof 1. is Thm. 14.23 in [204]; 2. is Cor. 14.30 in [204]; 3. is Thm. 16.23 in [204]; 4. is Exercise 16.16 in [204] (several variables) and Sect. 8.8 in [206] (algebraic extensions); 5. is Thm. 14.18 in [204]. ■

There was a time when designers of algorithms avoided the use of polynomial factorization. It was instead considered preferable if a problem could be solved "rationally", i.e., by only using the algorithms of Theorem 1.21 and of part 1 of Theorem 1.25. One motivation for this preference was that efficient polynomial factorization algorithms were not yet available, or they were only fast in theory but not yet in practice. This concern is nowadays no longer an issue. In this text, we will therefore take the freedom to apply polynomial factorization whenever it seems appropriate. However, it should be mentioned that there is a second motivation for preferring algorithms that do not involve polynomial factorization. The issue is that polynomial factorization inherently depends on the choice of the coefficient field C. For example, in contrast to the Euclidean algorithm, which applies for polynomials over any coefficient field, we do not have a general polynomial factorization algorithm and only know algorithms for certain fields C.

Example 1.26 The polynomial $p = x^4 + 2x^3 + 5x^2 + 4x + 1$ can be viewed as an element of various polynomial rings. Its factorizations look quite different depending on the choice. Here are some examples:

domain	factorization of p
$\mathbb{Z}_3[x]$	$(x^2 + x + 2)^2$
$\mathbb{Z}_5[x]$	$(x^2 + 2)(x^2 + 2x + 3)$
$\mathbb{Z}_{13}[x]$	$(x + 2)(x + 5)(x + 9)(x + 12)$
$\mathbb{Q}[x]$	$x^4 + 2x^3 + 5x^2 + 4x + 1$
$\mathbb{Q}(\sqrt{2})[x]$	$x^4 + 2x^3 + 5x^2 + 4x + 1$
$\mathbb{Q}(\sqrt{3})[x]$	$(x^2 + x + 2 + \sqrt{3})(x^2 + x + 2 - \sqrt{3})$
$\mathbb{Q}(\mathrm{i})[x]$	$(x^2 + (1 + 2\mathrm{i})x + \mathrm{i})(x^2 + (1 - 2\mathrm{i}) - \mathrm{i})$
$\mathbb{R}[x]$	$(x^2 + x + 3.73205\ldots)(x^2 + x + .267949\ldots)$
$\mathbb{C}[x]$	$(x + .5 + .13398\ldots\mathrm{i})(x + .5 - .13398\ldots\mathrm{i})$
	$\times(x + .5 - 1.86603\ldots\mathrm{i})(x + .5 + 1.86603\ldots\mathrm{i})$

□

Fortunately, efficient polynomial multiplication algorithms are known for most of the fields that tend to appear in the context of D-finite functions. The precise cost for factoring a polynomial depends again on the coefficient domain (and of course on the size of the input), some of the relevant bounds are stated in Theorem 1.25 above. It is important to keep in mind that polynomial factorization is much cheaper than integer factorization. At the time of writing, the best algorithm for factoring integers with n bits requires $\exp(\mathrm{O}(n^{1/3}\log(n)^{2/3}))$ bit operations. This is significantly more than the bounds appearing in Theorem 1.25. The algorithms discussed in this book do not use integer factorization.

Besides algorithms for integers and polynomials, we will also take for granted algorithms that solve classical problems in linear algebra. Also in this context, a multiplication time turns out to be of central importance.

Definition 1.27 A real number ω with $2 < \omega \leq 3$ is called a *matrix multiplication exponent* if for every field C there exists an algorithm which can multiply any two matrices in $C^{n\times n}$ using no more than $\mathrm{O}(n^\omega)$ operations in C. □

The classical matrix multiplication algorithm corresponds to $\omega = 3$, which is not optimal. Strassen's algorithm multiplies any two given $n \times n$ matrices using $\mathrm{O}(n^{\log_2(7)})$ operations in C. Note that $\log_2(7) \approx 2.80735 < 3$. This algorithm is used in practice for large matrices. Even smaller matrix multiplication exponents are known, but they are currently only of theoretical interest. It is not known what the smallest matrix multiplication exponent is. Whatever its value is, many other problems in linear algebra have the same cost.

Theorem 1.28 *There are algorithms which for any given $A \in C^{n\times n}$ compute the following data and require no more than $\mathrm{O}(n^\omega)$ operations in C:*

1. *the determinant* $\det(A)$*,*
2. *the inverse of A (if A is invertible),*
3. *the characteristic polynomial of A.*

There are algorithms which for any given $A \in C^{n\times m}$ *of rank r compute the following data and require no more than* $\mathrm{O}(nmr^{\omega-2})$ *operations in C:*

4. *the reduced echelon form of A,*
5. *a basis of the nullspace of A.* □

Proof 1. is Thm. 16.7 in [120]; 2. is Proposition 16.6 in [120]; 3. is Thm. 16.17 in [120]; 4. is shown in Sect. 2 of [179]; 5. follows directly from part 4. ■

Some questions about polynomials can be translated into linear algebra. For example, given $x_1, \ldots, x_n \in C$ pairwise distinct and $y_1, \ldots, y_n \in C$, the coefficients $c_0, \ldots, c_{n-1} \in C$ of the interpolation polynomial can be found by solving the linear system

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

The $n \times n$-matrix appearing here is called *Vandermonde matrix*. Its determinant turns out to be $\prod_{i<j}(x_j - x_i)$ and is therefore nonzero because the $x_1, \ldots, x_n$ are assumed to be pairwise distinct. Theorem 1.21 gives a lower cost for solving this linear system than Theorem 1.28 because the Vandermonde matrix has a specific structure which allows to solve the system more quickly.

Another example is related to the greatest common divisor of polynomials. Two polynomials

$$a = a_0 + \cdots + a_n x^n, \quad b = b_0 + \cdots + b_m x^m \in C[x]$$

are coprime if and only if there are $p, q \in C[x]$ such that $1 = ap + bq$. It can be shown that the degrees of p and q can be limited to $m - 1$ and $n - 1$, respectively. Therefore, we can find such p, q by solving the linear system

$$\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_m & & \ddots \\ a_n & & a_1 & & \ddots & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_n & & & b_m \end{pmatrix} \begin{pmatrix} p_0 \\ \vdots \\ p_{m-1} \\ q_0 \\ \vdots \\ q_{n-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}.$$

The matrix in this linear system is called the *Sylvester matrix* of a and b, its determinant is called the *resultant* of a and b and denoted by $\operatorname{res}(a, b)$. A key property is that two polynomials are coprime if and only if their resultant is nonzero.

For matrices with polynomial entries, it is clear that we can multiply two matrices of size $n \times n$ with polynomial entries of degree at most d using no more than $O(n^\omega M(d))$ operations in C. It does not immediately follow from the previous theorem that the same bound applies to other operations for polynomial matrices. When we directly apply the underlying algorithms to a polynomial matrix, viewed as a matrix over the function field $C(x)$, then the degrees of the matrix entries will grow so much during the computation that it affects the complexity. For example, if $A \in C[x]^{n\times n}$ has entries of degree d, the entries of A^{-1} (if it exists) are rational functions whose numerators and denominators may have degree up to nd, so even writing down all of the coefficients takes time proportional to $n^3 d$, which is more than $O(n^\omega M(d))$ if $\omega < 3$.

Theorem 1.29 *Let $A \in C[x]^{n\times m}$ be a matrix of rank r. Let $d_1, \ldots, d_m \in \mathbb{N}$ be such that all entries in the jth column have degree at most d_j ($j = 1, \ldots, m$). Let $d = d_1 + \cdots + d_m$ and let δ be the sum of the $r + 1$ largest integers among $d_1, \ldots, d_m$.*

1. *If $n = m$ then $\deg\det(A) \le d$.*
2. *If $n = m = r$ and $b \in C[x]^n$ is a vector with entries of degree at most $d_0 \in \mathbb{N}$, then the linear system $Ax = b$ has a unique solution $x \in C(x)^m$ whose jth component is a rational function $u/v \in C(x)$ with $\deg(u) \le d - d_j + d_0$ and $\deg(v) \le d$.*
3. *If $r < m$, then $\ker A \subseteq C(x)^m$ has a basis consisting of $m - r$ vectors in $C[x]^m$ whose jth components have degree at most $\delta - d_j$, for $j = 1, \ldots, m$.* □

Proof

1. This follows directly from the definition of the determinant.
2. By Cramer's rule, the jth coordinate of x is $\det(A^{(j)})/\det(A)$, where $A^{(j)}$ is the matrix obtained from A by replacing the jth column by b. Thus the degree bounds follow from part 1.
3. Without loss of generality, we may assume that $r = n$. (If not, discard redundant rows from A.) Write $a_1, \ldots, a_m$ for the columns of A. By the assumption on the rank, there are pairwise distinct indices $i_1, \ldots, i_r \in \{1, \ldots, m\}$ such that $a_{i_1}, \ldots, a_{i_r}$ are linearly independent over $C(x)$. Fix such indices and let $\tilde{A} = (a_{i_1}, \ldots, a_{i_r}) \in C[x]^{r\times r}$. For consistency, let the columns of $\tilde{A}$ be indexed by $i_1, \ldots, i_r$.
   For a $k \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_r\}$, consider the linear system $\tilde{A}\tilde{x} = -a_k$. If we index the coordinates of the solution vector $\tilde{x} \in C(x)^{m-1}$ in the same way as the columns of $\tilde{A}$, then Cramer's rule says that the jth coordinate of $\tilde{x} \in C(x)^{m-1}$ is $\det(\tilde{A}^{(j)})/\det(\tilde{A})$, for all $j \in \{i_1, \ldots, i_r\}$. Let $x \in C(x)^m$ be the vector which has the same entry as $\tilde{x}$ at the positions $j \in \{i_1, \ldots, i_r\}$, a 1 at position k, and zeros at the remaining positions $j \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_r, k\}$. For this vector, we have

$Ax = 0$ by construction. The vector $\det(\tilde{A})x \in \ker A$ has polynomial entries. The degree of its kth component is $\deg(\det(\tilde{A})) \leq (\sum_{\ell=1}^{r} d_{i_\ell}) + d_k - d_k \leq \delta - d_k$ by part 2, for $j \in \{i_1, \dots, i_r\}$, and the degree of the jth component is $\deg(\det(\tilde{A}^{(j)})) \leq (\sum_{\ell=1}^{r} d_{i_\ell}) + d_k - d_j \leq \delta - d_j$. For $j \in \{1, \dots, m\} \setminus \{i_1, \dots, i_r, k\}$, the jth component is 0, which also meets the required degree bound.

Summarizing, the construction described in the previous paragraph works for every $k \in \{1, \dots, m\} \setminus \{i_1, \dots, i_r\}$ and produces a set of $m - r$ linearly independent vectors with the announced degree bounds. ■

Note that we always have $\delta \leq d$, and that $\delta = d$ if $m = r + 1$. The degree bounds of parts 1 and 2 are not pessimistic but are almost always reached. The degree bound of part 3 is also tight for the particular nullspace basis considered in the proof. Unless there are better bases, this means that we are in a similar situation as with the computation of the inverse mentioned before: already the size of the output seems to force an undesirably large complexity for computing a nullspace basis of a polynomial matrix. Interestingly, it turns out that better bases do exist, and that they can be computed efficiently. This is stated in the following theorem, together with a bound on the cost of computing the determinant of a polynomial matrix.

Theorem 1.30

1. *There is an algorithm which for a given $A \in C[x]^{n \times n}$ with entries of degree at most d computes* $\det(A)$ *and which requires at most* $\mathrm{O}^{\sim}(n^{\omega} d)$ *operations in C.*
2. *There is an algorithm which for a given $A \in C[x]^{n \times m}$ of rank r with entries of degree at most d computes a basis of the nullspace* $\ker A$ *and which requires at most* $\mathrm{O}^{\sim}(nmr^{\omega-2} d)$ *operations in C.* □

Proof 1. is Prop. 41 in [414]; 2. is Theorem 7.3 in [415]. ■

Exercises

1. Suppose that $f(n) = \mathrm{O}(g(n))$ and $g(n) = \mathrm{O}(f(n))$. Which of the following statements follow?

- **a.** $f(n) = g(n)$ for all sufficiently large n;
- **b.** $f(n)/g(n)$ converges for $n \to \infty$;
- **c.** $\max(f(n), g(n)) = \mathrm{O}(\min(f(n), g(n)))$.

2. Show that $\log(n) = \mathrm{O}(n^{\epsilon})$ for every $\epsilon > 0$.

3. Make yourself comfortable with using a computer algebra system. For example, reproduce the computations of some of the examples in this section.

4. Is $\mathrm{O}^{\sim}(\log(n))$ the same as $\mathrm{O}^{\sim}(1)$?

5*. Show that the inequalities $\mathrm{M}(n)/n \geq \mathrm{M}(m)/m > 0$ $(n \geq m > 0)$ and $\mathrm{M}(mn) \leq m^2\,\mathrm{M}(n)$ $(n, m > 0)$ have the following consequences:

a. $\mathrm{M}(mn) \geq m\,\mathrm{M}(n)$;
b. $\mathrm{M}(n+m) \geq \mathrm{M}(n) + \mathrm{M}(m)$;
c. $\mathrm{M}(n) = \mathrm{O}(n^2)$;
d. $n = \mathrm{O}(\mathrm{M}(n))$;
e. $\mathrm{M}(cn) = \mathrm{O}(\mathrm{M}(n))$ for every fixed $c \in \mathbb{N}$.

6*. Let $T(n)$ be the number of operations a certain algorithm requires for input of size n. Suppose that $T(n) \leq 2T(n/2) + f(n)$ where $f(n) = \mathrm{O}(\mathrm{M}(n))$. Show that $T(n) = \mathrm{O}(\mathrm{M}(n)\log(n))$.

7. Let $p \in C[x]$ be a polynomial of degree n and let $k \in \mathbb{N}$. Show that p^k can be computed with no more than $\mathrm{O}(\mathrm{M}(kn))$ operations in C.

8. What is the cost of addition and multiplication in $\mathbb{Q}$ when rational numbers are represented by pairs of coprime integers?

9. Show that $\mathbb{Z}_m$ is not a field if m is not a prime.

10. Let $A = \begin{pmatrix} 3 & 5 \\ -5 & 7 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$ and $b = \begin{pmatrix} 4 \\ 1 \end{pmatrix} \in \mathbb{Q}^2$. Solve the linear system $Ax = b$ using homomorphic images with the primes 13, 17, 19, the Chinese remainder theorem, and rational reconstruction. Why does the approach fail with the primes 19, 23, 29?

11. What is the arithmetic complexity for finding the degree or extracting the coefficient of x^5 of a given polynomial?

12. Show that there is an algorithm which computes the product of any two polynomials $p, q \in C[x, y]$ with no more than $\mathrm{O}(\mathrm{M}(d_x d_y))$ operations in C, where $d_x = \max(\deg_x(p), \deg_x(q))$ and $d_y = \max(\deg_y(p), \deg_y(q))$.

13. Let R be a ring. The derivative of a polynomial $p \in R[x]$ is defined as the R-linear map $D\colon R[x] \to R[x]$ with $D(x^n) = nx^{n-1}$ for all $n \in \mathbb{N}$. For example, $D(x^4 + 2x - 5) = 4x^3 + 2$. What is the arithmetic complexity of computing $D(p)$ for a given $p \in R[x]$?

14*. According to part 3 of Theorem 1.21, we can compute $p(x+1)$ for any given $p(x) \in C[x]$ of degree n with $\mathrm{O}(\mathrm{M}(n))$ operations in C. Not using this knowledge, show that the other bounds stated in Theorem 1.21 imply that the problem can be solved with $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations in C.

Hint: Since we assume throughout that C has characteristic zero, it is in particular a field with infinitely many elements.

15. Show that there is an algorithm which for a given $p \in C[x]$ of degree n and a given $c \in C$ computes $p(c)$ using no more than $\mathrm{O}(n)$ operations in C.

16.** Show that $p \in C[x] \setminus C$ is squarefree if and only if $\gcd(p, p') = 1$, where p' refers to the derivative introduced in Exercise 13. Recall that C is a field of characteristic zero. Which direction works also in positive characteristic?

17. If $q \in C[x] \setminus C$ is irreducible, we have $\nu_q(p_1 p_2) = \nu_q(p_1) + \nu_q(p_2)$ for all $p_1, p_2 \in C[x]$. Does this relation already hold if q is just squarefree?

18. Let $\xi \in C$, let $r \in C(x)$, and let $f \in C((x - \xi))$ be the Laurent series associated to r. Show that $\nu_\xi(r) = \nu(f)$, where $\nu_\xi(r)$ is the valuation in $C(x)$ introduced in the present section and $\nu(f)$ is the order of Laurent series introduced in Sect. 1.1.

19. A rational function $u \in C(x)$ is called a *perfect square* if $u = v^2$ for some $v \in C(x)$. Design an algorithm which decides for any given $u \in C(x)$ whether it is a square. You may assume that C is algebraically closed, so that every element of C has a square root.

20. Use a computer algebra system to factor the polynomial $x^4 + 4x^3 - 8x - 1$, viewed as element of the following rings: **a.** $\mathbb{Z}_5[x]$; **b.** $\mathbb{Z}_7[x]$; **c.** $\mathbb{Z}_{31}[x]$; **d.** $\mathbb{Z}_{41}[x]$; **e.** $\mathbb{Q}[x]$; **f.** $\mathbb{Q}(\sqrt{2})[x]$; **g.** $\mathbb{Q}(\sqrt{3})[x]$; **h.** $\mathbb{Q}(\sqrt{5})[x]$.

21. Let $p \in C[x]$ be irreducible. Prove or disprove:

- **a.** $p(x + c)$ is irreducible for every $c \in C$.
- **b.** p' is irreducible.

22. Let $\alpha > 1$ be fixed. Show that the product of an $n \times n^\alpha$ matrix with an $n^\alpha \times n$ matrix can be computed using $\mathrm{O}(n^{\alpha+\omega-1})$ arithmetic operations.

References

The standard reference for computer algebra is currently the book of von zur Gathen and Gerhard [204]. Other general books on the subject are [65, 96, 120, 206, 280, 328, 476].

For the complexity estimates stated in this section, we tried to stick to the classical bounds that are in standard textbooks, even though there are better bounds available for some tasks. For example, Harvey and van der Hoeven recently showed [231] that $\mathrm{M}_{\mathbb{Z}}(n) = \mathrm{O}(n \log(n))$. However, for their algorithm to really be faster than the algorithm of Schönhage and Strassen [398], which for the first time showed $\mathrm{M}_{\mathbb{Z}}(n) = \mathrm{O}(n \log(n) \log\log(n))$ and held this record for more than three decades, n has to be unreasonably large. On the other hand, the algorithm of Schönhage and Strassen outperforms the classical multiplication algorithm already for integers of moderate lengths.

There is also an algorithm [232] for multiplying polynomials in $\mathbb{Z}_p[x]$ in a low bit complexity, but for polynomials in arbitrary coefficient rings, we have currently no better bound for the arithmetic complexity than $\mathrm{O}(n \log(n) \log\log(n))$. This bound is due to Cantor and Kaltofen [122], who give a polynomial analog of the Schönhage-Strassen algorithm.

There are also better bounds for polynomial factorization. For factorization in $\mathbb{Z}_p[x]$, Thm. 8.6 in [278] yields the bit complexity $\mathrm{O}^\sim(n^{3/2}m+nm^2)$ by replacing a subroutine for computing the composition of two polynomials modulo a third polynomial in the algorithm of Kaltofen and Shoup [255]. Note that this complexity is subquadratic, so this algorithm can factor polynomials more quickly than the school-book algorithm can multiply. For factorization in $\mathbb{Q}[x]$, the factorization algorithm of van Hoeij [447] achieves a complexity of $\mathrm{O}^\sim(n^2k^3(n+m))$ where k is the number of irreducible factors.

Matrix multiplication has undergone a long evolution since Strassen observed in the 1960s [416] that cubic complexity is not optimal. At the time of writing, the best known matrix multiplication exponent 2.37188 due to Duan, Wu and Zhou [177].

In order for computer algebra algorithms to be of any use, they have to be implemented in actual software. There are many computer algebra systems which provide an infrastructure for mathematical operations and some kind of programming language in order to apply and extend the provided functionality. One such system is Maple. Maple comes with a lot of add-on packages, some of which contain implementations of algorithms discussed in this book. Of particular relevance are the packages DETools, OreTools (contributed by Abramov, Le and Li [23]), gfun (contributed by Salvy and Zimmermann [379]), and Mgfun (contributed by Chyzak [154]).

Another general purpose computer algebra system is Mathematica. Mathematica does not have much built-in functionality for D-finite functions, but there are several useful third-party add-on packages. The state of the art for closure properties (cf. Sects. 2.3 and 3.3) and summation/integration (cf. Chap. 5) is Koutschan's package [289, 291]. Tools for guessing (cf. Sect. 1.5) can be found in a package by Kauers [262], and an implementation for finding generalized series solutions of recurrences (cf. Sect. 2.4) is available in another package of Kauers [263].

In Sage, the add-on package ore_algebra [277] contains implementations of many of the algorithms described in this book.

1.5 Guessing

Guessing is a popular technique for finding recurrence equations (or differential equations) of a D-finite sequence (or power series) about which we don't know more than the first few terms. For example, knowing that a sequence starts with $0, 1, 4, 9, 16, 25$, it is easily guessed that the sequence continues with $36, 49, 64$ and that the nth term is n^2, even though this is just a guess and the actual next term may just as well be $\sqrt{\pi}$. The guess is based on the observation that the first terms follow a simple pattern, and in absence of further knowledge about the sequence it is only the simplicity of the pattern relative to the number of matched terms that lets the pattern appear plausible. The pattern $n^6-15n^5+85n^4-225n^3+275n^2-120n$

also matches the first six terms, but it is less convincing because it is less simple, and if we had been given only the terms $0, 1, 4$, the pattern n^2 would not be as convincing as when we know that it matches twice as many terms.

If the sequence $(a_n)_{n=0}^{\infty}$ can be described by a polynomial p, then we can find p by interpolation (Theorem 1.21). The interpolating polynomial of the first $N+1$ terms $a_0, \dots, a_N$ of the sequence is the unique polynomial q of degree at most N with $q(n) = a_n$ for $n = 0, \dots, N$. For every N that exceeds the degree of p, uniqueness implies that $p = q$, so if we know (a bound on) the degree of p, then we can recover p by supplying sufficiently many terms. If we have no clue about the degree, we can still compute interpolating polynomials for $a_0, \dots, a_N$ for increasing choices of N. Eventually the sequence of interpolating polynomials will stabilize, and whenever we get the same polynomial a few times in a row, this is evidence that we have found p. More directly, whenever the degree of an interpolating polynomial q is less than N, we can hope to have $p = q$, and in a sense, the hope gets more and more justified when we let $N - \deg q$ grow.

The purpose of this section is to generalize this reasoning from polynomials to D-finite recurrences or differential equations. Given a finite number of terms $a_0, \dots, a_N$, we want to determine linear recurrence equations with polynomial coefficients matching this data, or linear differential equations with polynomial coefficients satisfied by formal power series whose first coefficients are $a_0, \dots, a_N$. Some of the algorithms discussed in later chapters use these techniques as subroutines, with a suitable choice of N that ensures that the resulting equations are indeed correct. But even if no such N is known, guessing is one of the first things to do when we face a sequence or power series for which we can compute the first terms and which we suspect to be D-finite.

For reconstructing a recurrence or differential equation from a given finite number of terms, we first have to choose the order r of the desired equation and the degree d of its polynomial coefficients. For a sequence $(a_n)_{n=0}^{\infty}$, the task is then to compute the polynomial vectors $(p_0, \dots, p_r) \in C[x]^{r+1}$ with $\deg_x p_i \leq d$ for all i such that $p_0(n)a_n + \dots + p_r(n)a_{n+r} = 0$ for all n in question. Note that the set of all these vectors forms a C-vector space of dimension at most $(r+1)(d+1)$.

In the differential case we consider a formal power series $a(x) = \sum_{n=0}^{\infty} a_n x^n$ for which the first few terms are known. To satisfy a differential equation $p_0(x)a(x) + \dots + p_r(x)a^{(r)}(x) = 0$ with polynomial coefficients $p_0, \dots, p_r$ means that $p_0(x)a(x) + \dots + p_r(x)a^{(r)}(x)$ is the zero power series, i.e., for all $n \in \mathbb{N}$ the coefficient of x^n in $p_0(x)a(x) + \dots + p_r(x)a^{(r)}(x)$ is zero. Given r and d and a finite number of initial terms of $a(x)$, the task is then to find all polynomial vectors $(p_0, \dots, p_r) \in C[x]^{r+1}$ with $\deg_x p_i \leq d$ for all i such that the first few coefficients of the formal power series $p_0(x)a(x) + \dots + p_r(x)a^{(r)}(x)$ are zero.

In the analogy with polynomial interpolation, the following theorem corresponds to the fact that fitting a polynomial p of degree d through $N+1$ given values will always work when $d \geq N$.

Theorem 1.31 *Let $a_0, \dots, a_N \in C$ and $r, d \in \mathbb{N}$.*

1. *Let* $V \subseteq C[x]^{r+1}$ *be the* C*-vector space of all* $(r+1)$*-tuples* $(p_0, \ldots, p_r)$ *with* $\deg p_i \leq d$ *for* $i = 0, \ldots, r$ *such that*

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$$

for $n = 0, \ldots, N-r$. *Then* $\dim_C V \geq (r+1)(d+2) - N - 2$.

2. *Let* $V \subseteq C[x]^{r+1}$ *be the* C*-vector space of all* $(r+1)$*-tuples* $(p_0, \ldots, p_r)$ *with* $\deg p_i \leq d$ *for* $i = 0, \ldots, r$ *such that*

$$x^{N-r+1} \mid p_0(x)a(x) + p_1(x)a'(x) + \cdots + p_r(x)a^{(r)}(x),$$

where $a(x) = a_0 + a_1x + \cdots + a_Nx^N$. *Then* $\dim_C V \geq (r+1)(d+2) - N - 2$. □

Proof Part 1 is Exercise 1. We show part 2. Write $p_i = \sum_{j=0}^{d} p_{i,j}x^j$ for $i = 0, \ldots, r$ with undetermined coefficients $p_{i,j}$. Then $p_0(x)a(x) + p_1(x)a'(x) + \cdots + p_r(x)a^{(r)}(x)$ is a polynomial in x whose coefficients are linear combinations of the undetermined coefficients $p_{i,j}$. Equating the coefficients of the terms x^k with $k \leq N - r$ to zero gives a homogeneous linear system with $N - r + 1$ equations and $(r+1)(d+1)$ variables. The solution space of such a system has dimension at least $(r+1)(d+1) - (N-r+1)$. ■

The recurrences and differential equations predicted by the theorem above exist regardless of the choice of $a_0, \ldots, a_N$, and therefore they should not be taken as evidence that $a_0, \ldots, a_N$ are the first terms of a D-finite object. The theorem corresponds to the fact that for any $N + 1$ numbers there exists an interpolating polynomial of degree at most N. The condition that the degree is smaller than expected corresponds to cases when the dimension of V is strictly larger than the stated lower bounds. In these cases, V will typically contain some generic equations as well as some that exist only because of a particular structure in the data. By choosing r, d such that $N \geq (r+1)(d+2) - 2$ we can ensure that V only contains such interesting equations.

In practice, these interesting equations are good candidates for equations that may hold beyond the first few terms for the entire infinite sequence or power series under consideration. If for some fixed choice r, d we write V_N for the vector spaces of Theorem 1.31 for varying choices of N, then we have $V_N \supseteq V_{N+1}$ for every N, and $V_\infty := \bigcap_{N=0}^{\infty} V_N$ is precisely the vector space of all equations that hold for the infinite object. As all of the vector spaces have dimension at most $(r+1)(d+1) < \infty$, the chain $V_N \supseteq V_{N+1} \supseteq V_{N+2} \supseteq \cdots$ must eventually stabilize, so we will have $V_N = V_\infty$ for all sufficiently large N. The following examples reflect the typical situation where we have $V_\infty = V_{(r+1)(d+2)-2}$.

Example 1.32

1. Consider the sequence $(a_n)_{n=0}^{\infty}$ with $a_n = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}$. Suppose we only know the terms a_n for $n = 0, \ldots, 7$. These are 1, 3, 13, 63, 321, 1683, 8989,

48639. This data suffices to search for recurrences of order $r = 2$ and degree $d = 1$. Any recurrence of the form

$$(c_{0,0} + c_{0,1}n)a_n + (c_{1,0} + c_{1,1}n)a_{n+1} + (c_{2,0} + c_{2,1}n)a_{n+2} = 0$$

valid for all $n \in \mathbb{N}$ must hold in particular for $n = 0, \ldots, 7-2 = 5$. Substituting these indices into the equation and using the known first terms of the sequence yields a homogeneous linear system of $7 - 2 + 1 = 6$ equations for the $(2 + 1)(1 + 1) = 6$ unknowns $c_{i,j}$:

$$\begin{aligned}
c_{0,0} \quad\quad & + 3c_{1,0} & & + 13c_{2,0} & & = 0,\\
3c_{0,0} + 3c_{0,1} & + 13c_{1,0} & + 13c_{1,1} & + 63c_{2,0} & + 63c_{2,1} & = 0,\\
13c_{0,0} + 26c_{0,1} & + 63c_{1,0} & + 126c_{1,1} & + 321c_{2,0} & + 642c_{2,1} & = 0,\\
63c_{0,0} + 189c_{0,1} & + 321c_{1,0} & + 963c_{1,1} & + 1683c_{2,0} & + 5049c_{2,1} & = 0,\\
321c_{0,0} + 1284c_{0,1} & + 1683c_{1,0} & + 6732c_{1,1} & + 8989c_{2,0} & + 35956c_{2,1} & = 0,\\
1683c_{0,0} + 8415c_{0,1} & + 8989c_{1,0} & + 44945c_{1,1} & + 48639c_{2,0} & + 243195c_{2,1} & = 0.
\end{aligned}$$

This linear system has a solution space of dimension one which corresponds to the recurrence

$$(1 + n)a_n - (9 + 6n)a_{n+1} + (2 + n)a_{n+2} = 0$$

and all of its constant multiples. By construction, this recurrence holds for $n = 0, \ldots, 5$. In fact it holds for all $n \in \mathbb{N}$, but this fact can obviously not be proven if we know nothing more about the sequence except the terms $a_0, \ldots, a_7$. With the methods of Chap. 5, the correctness of the recurrence for all $n \in \mathbb{N}$ can be proven based on the sum representation of $(a_n)_{n=0}^{\infty}$.

2. Let $(a_n)_{n=0}^{\infty}$ be as before and consider the formal power series $a(x) = \sum_{n=0}^{\infty} a_n x^n$. The terms $a_0, \ldots, a_6$ suffice to search for linear differential equations of order $r = 1$ with polynomial coefficients of degree $d = 2$. For any differential equation

$$(c_{0,0} + c_{0,1}x + c_{0,2}x^2)a(x) + (c_{1,0} + c_{1,1}x + c_{1,2}x^2)a'(x) = 0$$

we must have

$$\begin{aligned}
&(c_{0,0} + c_{0,1}x + c_{0,2}x^2)(1 + 3x + 13x^2 + 63x^3\\
&\qquad + 321x^4 + 1683x^5 + 8989x^6 + \cdots)\\
&+ (c_{1,0} + c_{1,1}x + c_{1,2}x^2)(3 + 26x + 189x^2 + 1284x^3\\
&\qquad + 8415x^4 + 53934x^5 + \cdots)
\end{aligned}$$

$$
\begin{aligned}
&= (c_{0,0} + 3c_{1,0}) + (3c_{0,0} + c_{0,1} + 26c_{1,0} + 3c_{1,1})x \\
&\quad + (13c_{0,0} + 3c_{0,1} + c_{0,2} + 189c_{1,0} + 26c_{1,1} + 3c_{1,2})x^2 \\
&\quad + (63c_{0,0} + 13c_{0,1} + 3c_{0,2} + 1284c_{1,0} + 189c_{1,1} + 26c_{1,2})x^3 \\
&\quad + (321c_{0,0} + 63c_{0,1} + 13c_{0,2} + 8415c_{1,0} + 1284c_{1,1} + 189c_{1,2})x^4 \\
&\quad + (1683c_{0,0}+321c_{0,1}+63c_{0,2}+53934c_{1,0} + 8415c_{1,1} + 1284c_{1,2})x^5 + \cdots \\
&= 0 + 0x + 0x^2 + 0x^3 + 0x^4 + 0x^5 + \cdots
\end{aligned}
$$

where the dots contain only higher order terms. Comparing coefficients of x^i for $i = 0, \dots, 5$ leads again to a homogeneous linear system with 6 equations for the $(1 + 1)(2 + 1) = 6$ variables $c_{i,j}$. The system has a solution space of dimension one generated by a solution corresponding to the differential equation

$$(-3 + x)a(x) + (1 - 6x + x^2)a'(x) = 0.$$

This equation is indeed correct.

3. Consider the sequence $(p_n)_{n=0}^{\infty}$ where $p_0 = 1$ and p_n is the nth prime number for $n \geq 1$. Using the terms $p_0, \dots, p_{10}$, we can search as before for potential recurrence equations of order $r = 2$ and degree $d = 2$, and we find that $V_{10} = \{0\}$ in this case. This proves that the infinite sequence of primes does not satisfy any linear recurrence of order at most 2 with polynomial coefficients of degree at most 2.
   Using a sufficiently large number of terms, it can be shown that there is also no recurrence of order at most 10 and degree at most 10, or of order at most 100 and degree at most 100, but other techniques are needed to prove that $(p_n)_{n=0}^{\infty}$ does not satisfy any linear recurrence with polynomial coefficients at all. □

As can be seen in these examples, recurrences and differential equations can be found by linear algebra when sufficiently many initial terms are known. The general idea is to make an ansatz with undetermined coefficients, then derive linear constraints by fitting the given data to the ansatz, and then solve a homogeneous linear system. A quick-and-dirty implementation in a general purpose computer algebra system like Maple or Mathematica won't require much more than two or three lines of code, and it would be enough to handle examples like those above. For larger examples, one should make sure to avoid unnecessary recomputations when setting up the linear systems. A straightforward way to do so is given in the following two algorithms.

Algorithm 1.33
Input: *Two nonnegative integers r, d, an array $a_0, \dots, a_N$ of elements of a field C.*
Output: *A basis for the vector space $V_N \subseteq C[x]^{r+1}$ of all polynomial vectors $(p_0, \dots, p_r)$ with components of degree at most d such that $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ for $n = 0, \dots, N - r$.*

Let M be a matrix over C with $N-r+1$ rows and $(r+1)(d+1)$ columns.
for $n = 0, \dots, N-r$ do
  for $i = 0, \dots, r$ do
    Set $M[n,i]$ to a_{n+i}.
for $j = 1, \dots, d$ do
  for $n = 0, \dots, N-r$ do
    for $i = 0, \dots, r$ do
      Set $M[n,(r+1)j+i]$ to $n\,M[n,(r+1)(j-1)+i]$.
Compute a basis B of the space of all $v \in C^{(r+1)(d+1)}$ with $Mv = 0$.
for each $(b_0, \dots, b_{(r+1)(d+1)-1}) \in B$ do
  Output $\left(\sum_{j=0}^{d} b_{(r+1)j}x^j,\ \sum_{j=0}^{d} b_{(r+1)j+1}x^j, \dots, \sum_{j=0}^{d} b_{(r+1)j+r}x^j\right) \in C[x]^{r+1}$.

Algorithm 1.34
Input: *Two nonnegative integers r, d and a polynomial $a(x) = a_0 + a_1x + \cdots + a_Nx^N$ with coefficients in a field C.*
Output: *A basis for the vector space $V_N \subseteq C[x]^{r+1}$ of all polynomial vectors $(p_0, \dots, p_r)$ with components of degree at most d such that $x^{N-r+1} \mid p_0(x)a(x) + \cdots + p_r(x)a^{(r)}(x)$.*

Let M be a matrix over C with $N+1$ rows and $(r+1)(d+1)$ columns.
for $n = 0, \dots, N$ do
  Set $M[n,0]$ to a_n.
for $i = 1, \dots, r$ do
  for $n = 0, \dots, N-i$ do
    Set $M[n,i]$ to $(n+1)\,M[n+1,i-1]$.
Discard the rows $M[N-r+1,*], \dots, M[N,*]$ from M.
for $j = 1, \dots, d$ do
  for $i = 0, \dots, r$ do
    for $n = 0, \dots, N-r$ do
      Set $M[n,(r+1)j+i]$ to $M[n-j,i]$ if $j \geq n$ and to 0 otherwise.
Compute a basis B of the space of all $v \in C^{(r+1)(d+1)}$ with $Mv = 0$.
for each $(b_0, \dots, b_{(r+1)(d+1)-1}) \in B$ do
  Output $\left(\sum_{j=0}^{d} b_{(r+1)j}x^j,\ \sum_{j=0}^{d} b_{(r+1)j+1}x^j, \dots, \sum_{j=0}^{d} b_{(r+1)j+r}x^j\right) \in C[x]^{r+1}$.

Theorem 1.35 *Algorithms 1.33 and 1.34 are correct, and the cost is dominated by the cost of computing a basis of the nullspace of a matrix with $N-r+1$ rows and $(r+1)(d+1)$ columns. In particular, if $N = (r+1)(d+1) + \mathrm{O}(1)$, then both algorithms require $\mathrm{O}(r^\omega d^\omega)$ operations in C.* □

Proof For the correctness it suffices to observe that the matrices M are set up in such a way that finally $M[n, j(r+1)+i]$ is precisely $n^j a_{n+i}$ in Algorithm 1.33 and the coefficient of x^n in $x^j a^{(i)}(x)$ in Algorithm 1.34.

For the cost estimate, note that in both algorithms the construction of M takes at most $(d+1)(r+1)(N-r+1) = \mathrm{O}(d^2 r^2)$ operations, and that a nullspace basis of an $(N-r+1) \times (r+1)(d+1)$ matrix can be computed using $\mathrm{O}(d^\omega r^\omega)$ operations. ■

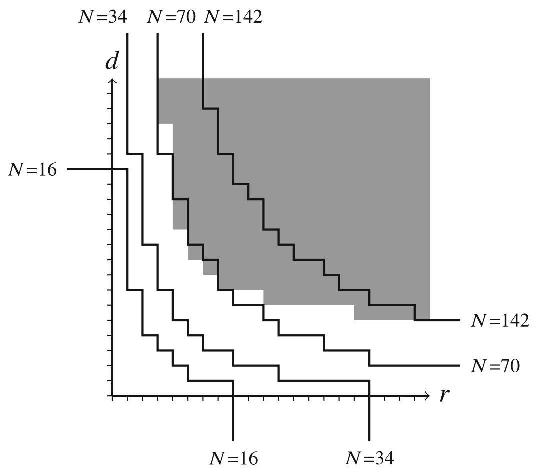
Algorithms 1.33 and 1.34 work for any choice of r, d, N, but the results are interesting only if $N \geq (r+1)(d+2)-2$. Typical implementations therefore contain an additional instruction at the beginning which aborts with an error message "not enough data" if $N < (r+1)(d+2)-2$.

If the number of known terms is fixed, then only a certain finite set of points (r, d) can be reasonably tested for possible recurrences or differential equations. It is instructive to compare the location of these points to the location of the points (r, d) for which there actually exist equations.

Example 1.36 The formal power series

$$\frac{1+x^5}{\sqrt{x+1}} + \frac{2x+3}{\sqrt{1-x}} + (3x^4 - 4x^3 + 8)\exp\left(\frac{x}{1-x}\right) = 12 + 11x + \tfrac{29}{2}x^2 + \cdots$$

satisfies a differential equation of order r with polynomial coefficients of degree d for every point (r, d) in the gray region in the figure below.



From the $N+1$ coefficients $a_0, \ldots, a_N$ of the series, such an equation can be reconstructed if $N \geq (r+1)(d+2)-2$. For some choices of N, the regions which can be investigated are those underneath the black curves in the figure. All of these regions are finite, but only the region for $N = 16$ completely fits into the picture. For $N = 16$ and $N = 34$ no equations can be found. In the case $N = 70$ we can recover all of the equations with $(r, d) \in \{(4, 11), (4, 12), (4, 13), (5, 9), (5, 10), (6, 8), (6, 9), (7, 7)\}$, but all other equations are out of reach, because if we apply the algorithm with $(r, d) = (3, 18)$, say, it would return a solution space which contains some right and some wrong equations, and it is not clear how to distinguish them. With $N = 142$, a greater portion of the gray region is covered, including the point $(3, 18)$. $\square$

While an equation is always unreliable if $N < (r + 1)(d + 2) - 2$, there is no guarantee that an equation can be trusted whenever $N \geq (r + 1)(d + 2) - 2$. No finite number of terms will suffice to draw conclusions about the whole formal power series or infinite sequence in question, but there are some tests which can be used to get some idea as to how trustworthy a guessed equation is. One way to increase the confidence into a guess is to increase, if possible, the number of terms. The larger the difference $(N - r + 1) - (r + 1)(d + 1)$, the harder it is for an overdetermined linear system with $(r + 1)(d + 1)$ variables and $N - r + 1$ equations to accidentally have a solution. A second test is to look at the integers appearing in the equation. Good equations typically only contain integers which are roughly as long as (or even considerably shorter than) the integers in the input data, whereas bad equations typically contain integers which are much longer than that. Third, for guessed recurrences of integer sequences one can use the recurrence to calculate some further terms and see whether they all are integers. A fourth test is to check the equation for certain algebraic properties which are "meaningful," that is, properties such equations would typically have but which are very unlikely for random equations. For example, good equations typically have a leading coefficient polynomial with several low-degree factors, while this is not to be expected for a false guess. Similarly, good equations are often Fuchsian (cf. Definition 3.40) while bad equations are usually not.

In applications, equations of minimal order are usually more interesting than equations of higher order and smaller degree. It is also often the case that although higher order equations may have lower degree, their total size is still much larger than the total size of the minimal-order equation because the coefficients of the polynomials in the equation tend to be much longer for higher order equations of lower degree. If the number of available terms is not sufficient to catch the minimal-order equation, it is therefore advisable to compute an equation of possibly non-minimal order, then use this equation to generate more data, and then try again to construct the minimal-order equation taking into account these additional terms. This approach works best in combination with the technique of homomorphic images (cf. parts 3, 4 and 5 of Theorem 1.16 or parts 4, 5 and 6 of Theorem 1.21, respectively). Many algorithms discussed in this book can and should be implemented using homomorphic images in order to avoid unnecessary intermediate expression swell. For most of the algorithms, this can be regarded as an implementation detail which is independent of the understanding of how the algorithm works or how to apply it. Despite its importance for the performance, we will therefore not always emphasize the option of using homomorphic images in later chapters. In the context of guessing however, it seems worthwhile to make some remarks related to the use of homomorphic images, because the best way to employ the technique cannot be encapsulated into some general purpose implementation but requires some interaction by the user.

Suppose we are given $N+1$ elements $a_0, \dots, a_N$ of a ring R in which calculations are expensive. We want to find candidate operators $L \in R[x][S]$ of order r and degree d annihilating the infinite sequence $(a_n)_{n=0}^{\infty}$. Rather than applying Algorithm 1.33 to $a_0, \dots, a_N$, we choose a ring R' in which calculations are cheaper and a ring homomorphism $\phi\colon R \to R'$, and apply Algorithm 1.33 to $\phi(a_0), \dots, \phi(a_N)$ to find candidate operators in $R'[x][S]$. Depending on how the $a_0, \dots, a_N$ were obtained in the first place, it may be advisable to directly compute only their images under ϕ instead of the actual terms (in fact the generation of terms often takes more time than the guessing). The first feature of using homomorphic images is: if no recurrence is found for the images $\phi(a_i)$, then no recurrence can be found for the a_i.

Example 1.37 We want to show that $(a_n)_{n=0}^{\infty}$ with $a_n = 5^{\binom{n}{5}}$ does not satisfy any recurrence of order ≤ 5 and degree ≤ 20. On the author's computer, computing the terms $a_0, \dots, a_{131}$ explicitly takes more than two minutes. The last of these terms is an integer with 208015329 decimal digits. Computing $\phi(a_0), \dots, \phi(a_{131})$ where $\phi\colon \mathbb{Z} \to \mathbb{Z}_{97}$ is the natural homomorphism requires less than a millisecond. Using these homomorphic images, we can use Algorithm 1.33 to search for a recurrence of order 5 and degree 20 over the constant field $\mathbb{Z}_{97}$. It turns out that there is none. This implies that the original sequence does not satisfy any recurrence of order 5 and degree 20 with integer coefficients, for if it did, then we could ensure that not all of the integer coefficients of the recurrence are multiples of 97 by canceling the common factors. Applying ϕ to all of the coefficients of the result would yield a nontrivial recurrence for the sequence $(\phi(a_n))_{n=0}^{\infty}$. □

The same reasoning applies to sequences in $\mathbb{Q}$ if a modulus p is chosen which does not divide any of the denominators of the given finitely many terms. For sequences in an algebraic number field $\mathbb{Q}(\alpha)$, choose a prime p which avoids the denominators in the given terms and which also has the property that the minimal polynomial $f \in \mathbb{Z}[x]$ of α admits a factorization with at least one linear factor when viewed as a polynomial in $\mathbb{Z}_p[x]$. Then α can be mapped to such a root. For sequences in a polynomial ring $C[t]$, we can map t to any element of C, and for sequences in a rational function field $C(t)$, we can map t to any element of C that avoids the roots of all appearing denominators.

The second feature of using homomorphic images is: if for a sufficiently large modulus we have found an equation for the homomorphic images, then we can reconstruct from it an equation for the original sequence. In general it will not suffice to just pick a representative in $\{-\lfloor m/2 \rfloor, \dots, \lfloor m/2 \rfloor\}$ for each element of $\mathbb{Z}_m$, because every constant multiple of a correct equation is again a correct equation, and we cannot hope that the modular equation accidentally has such a constant factor for which the integers in the preimage have only a small number of digits. In order to eliminate any such disturbing constant factors, we can divide the modular equation by one of its nonzero coefficients. This changes this particular coefficient to one and all of the other coefficients to homomorphic images of rational numbers. We can then use rational reconstruction (cf. Theorem 1.16) to recover these rational numbers from their images.

Example 1.38 Consider the sequence $(a_n)_{n=0}^{\infty}$ with $a_n = n(\frac{5}{7})^n$. The corresponding sequence modulo 45007 starts as 0, 25719, 43171, 10892, 40378. From these terms we can find the operator $4581(n+1) + 2588nS$, which is correct for the sequence of homomorphic images, but not for the original sequence if we read 4581 and 2588 as integers. Applying rational reconstruction to 4581 and 2588 gives $-\frac{92}{167}$ and $\frac{121}{87}$, respectively, which however does not correspond to a valid recurrence either. Multiplying the operator by $\frac{1}{2588}$ gives $19288(n+1) + nS$ (because $\frac{4581}{2588} \equiv 19288 \bmod 45007$), and rational reconstruction finds that $19288 \equiv -\frac{5}{7} \bmod 45007$. This is the correct result. □

Rational reconstruction can also be used if for some choice of r and d there are several linearly independent solutions. In this case, instead of dividing by some nonzero coefficient, one should bring the basis of the solution space into some canonical form.

Every correct operator can be recovered from its homomorphic image if the modulus is sufficiently large. If we know in advance how long the coefficients in the true operators can get, we can choose the modulus accordingly. But we don't need to have such a bound. This is the third feature of using homomorphic images: since we can use the Chinese remainder theorem (Theorem 1.16) to merge homomorphic images, we do not need to discard the result of a computation with a modulus that turned out to be too small. Instead, we can keep repeating the computation for more and more small moduli and merge them all into one large homomorphic image until the combined modulus is large enough to allow for rational reconstruction to succeed.

Example 1.39 For the power series $a(x) = (1+4x)^{1/5} + (1-2x)^{1/7}$ we can find the following two differential equations modulo 1091 and 1097, respectively:

$$
\begin{aligned}
&(x^3 + 952x^2 + 921x + 256)a''(x) \\
&\quad + (63x^2 + 791x + 1000)a'(x) + (904x + 990)a(x) = 0, \\
&(x^3 + 683x^2 + 309x + 86)a''(x) \\
&\quad + (32x^2 + 670x + 743)a'(x) + (1003x + 635)a(x) = 0.
\end{aligned}
$$

Both are normalized so that the coefficient of $x^3a''(x)$ is 1, but rational reconstruction gives incorrect results in both cases. Using the Chinese remainder theorem, we can find the following differential equation modulo $1091 \cdot 1097 = 1196827$:

$$(x^3 + 1047221x^2 + 112203x + 430110)a''(x)$$
$$+ (205171x^2 + 222264x + 1045087)a'(x) + (581316x + 265012)a(x) = 0.$$

Rational reconstruction applied to the coefficients of this equation yields

$$(x^3 - \tfrac{21}{8}x^2 + \tfrac{15}{32}x + \tfrac{19}{64})a''(x) + (\tfrac{23}{35}x^2 - \tfrac{271}{70}x + \tfrac{317}{560})a'(x) + (\tfrac{1}{35}x + \tfrac{43}{140})a(x) = 0.$$

This equation is correct. □

In practice, it is best to use moduli which are close to, but not larger than, the word size of the processor, so that the computer algebra system can exploit fast hardware instructions for the arithmetic and does not need to fall back on comparatively slow code for long integer arithmetic. For polynomials, take moduli of the form $x - c$ for pairwise distinct constants c from the ground field and use the algorithms of Theorem 1.21 instead of those of Theorem 1.16. It is also a good idea to handle different moduli in parallel on different processors (or even on different computers).

In many nontrivial applications, the generation of data needs much more time than guessing an equation. Of course, when we use guessing to search for equations, we typically do not already know a recurrence or a differential equation that could be used to compute many terms efficiently. It is therefore important to note that it is often sufficient to compute the terms only modulo a few primes. The number of primes needed depends on the lengths of the coefficients of the equation, and not on the length of the terms entering into the computation. For example, guessing the equations in Example 1.39 requires the terms $a_0, \dots, a_{13}$, and we succeeded to recover the true differential equation using only the primes 1091 and 1097, but it is impossible to reconstruct the term $a_{13} = \frac{1109168538109383975328181452\,8}{20697725611846923828125}$ from its images modulo these two primes.

Here are two more ideas which can significantly improve the overall performance:

- *Trading order for degree.* Assuming that the generation of data is expensive compared to the guessing, we will try to minimize the number of terms needed. At the same time, the number of moduli needed in order to reconstruct an equation from its homomorphic images is proportional to the length of the coefficients in this equation, so we would prefer to compute an equation with short coefficients. Typically, the equation of minimal order has short coefficients but large degree polynomials, so that N is not optimal. On the other hand, equations for which N is minimal tend to have extremely lengthy coefficients.

  To achieve a balance on both ends, we can guess the homomorphic image of an equation which can be found with a small N, then use this equation to efficiently generate further terms in $\mathbb{Z}_p$, then use these terms to guess a minimal order equation, and lastly apply the Chinese remainder theorem and rational reconstruction on them. Alternatively, we could also guess several linearly independent equations for which N is small and then compute the greatest common right divisor of the corresponding operators (cf. Sect. 4.2). With high probability, this operator corresponds to the minimal order equation.

- *Unbalanced rational reconstruction.* We are free to decide which of the nonzero coefficients we use for normalization. Some choices are better than others, because in typical examples the length of the coefficients varies in different parts of the equation. A good choice seems to be the leading coefficient of the leading coefficient, because this coefficient tends to be one of the shortest coefficients in the equation. By using it for the normalization, we have a reason to expect that the preimages of the rational reconstruction are fractions with shorter denominators than numerators. This expectation can be exploited by the rational reconstruction algorithm.

  Moreover, when the reconstruction of the whole equation fails because we did not use enough moduli to recover the longest coefficients, there is a good chance that we have already successfully recovered some of the small ones. If we are lucky, the least common multiple of all of the trustworthy denominators is already the common denominator of the whole equation. If so, we can multiply the whole equation by this denominator. Then for finding the remaining long coefficients, we don't need to apply rational reconstruction any more but only the Chinese remainder theorem.

An implementation of guessing using homomorphic images which takes into account the first of these two suggestions would proceed roughly as follows.

Algorithm 1.40
Input: *An infinite sequence* $(a_n)_{n=0}^{\infty}$ *or a formal power series* $a(x) = \sum_{n=0}^{\infty} a_n x^n$ *with* $a_n \in \mathbb{Q}$ *for all* $n \in \mathbb{N}$, *specified by some procedure that computes for every given* $n \in \mathbb{N}$ *and* $p \in \mathbb{N}$ *the homomorphic image of* a_n *in* $\mathbb{Z}_p$, *if it exists, and raises an error if not.*
Output: *A guessed recurrence for* $(a_n)_{n=0}^{\infty}$ *or a guessed differential equation for* $a(x)$. *The output is only guaranteed to match a finite number of the first terms of* $(a_n)_{n=0}^{\infty}$ *or* $a(x)$. *The algorithm may run forever if no equation exists.*

1 *Set* $r = d = 2$ *and choose a prime* p.
2 *while no equation has been found do*
3   *Increase* r, d, *e.g., set* $r = 2r; d = 4d$.
4   *Compute the first* $(r+1)(d+2)+10$ *terms modulo* p. *If this yields an error, replace* p *by another prime and try again.*
5   *Use Algorithm 1.33 or 1.34 or 1.50 to search for possible equations of order* $\leq r$ *and degree* $\leq d$ *with* $C = \mathbb{Z}_p$.
6 *Use the discovered equation(s) from step 5 to generate some further terms modulo* p.
7 *Use the terms from step 6 to search for some pair* (r_0, d_0) *such that guessing finds an equation of order* r_0 *and degree* d_0 *and* $(r_0+1)(d_0+2)$ *is as small as possible.*

8 *Search for some pair* (r_1, d_1) *such that guessing finds an equation of order* r_1 *and degree* d_1 *and* r_1 *is as small as possible. Alternatively, calculate the greatest common right divisor of all of the operators found for order* r *and degree* d *and let* r_1 *be the order of this operator.*

9 *Let* $m = p$ *and let* L_m *be the operator of order* r_1 *normalized so that the leading coefficient of the leading coefficient is* 1.

10 *Repeat the following steps:*

11   *Choose several new primes, say* $p_1, \dots, p_\ell$.

12   *for all* $i = 1, \dots, \ell$ *in parallel do*

13   *Compute* $(r_0 + 1)(d_0 + 2) + 10$ *terms of* $(a_n)_{n=0}^{\infty}$ *modulo* p_i. *If this yields an error, mark the prime* p_i *as "discarded".*

14   *Use the terms from step 13 to guess an equation of order* r_0 *and degree* d_0.

15   *Use the equation from step 14 to obtain an equation of order* r_1 *(either by generating more terms and guessing, or by computing a greatest common right divisor).*

16   *Let* L_{p_i} *be the resulting operator, normalized so that the leading coefficient of the leading coefficient is* 1.

17   *Merge* $L_{p_1}, \dots, L_{p_\ell}$ *using the Chinese remainder theorem into an operator* L_q *valid modulo* $q := p_1 \cdots p_\ell$. *Omit the primes that have been marked as "discarded".*

18   *Merge* L_m *and* L_q *into a new operator, again called* L_m, *and set* $m := q\,m$.

19   *Apply rational reconstruction to the coefficients in* L_m *and call the resulting operator* L.

20   *Pick a new prime* p *and compute the first few terms of* $(a_n)_{n=0}^{\infty}$ *or* $a(x)$ *modulo* p.

21   *If* L *matches the terms in step 19 (mod* p*), output* L *and stop, otherwise go back to step 11.*

Exercises

1. Show part 1 of Theorem 1.31.

2. Let $(a_n)_{n=0}^{\infty}$ be an infinite sequence. Assume that it satisfies a recurrence of order 2 with polynomial coefficients of degree 2. Assume further that the first terms of the sequence are 2, 1, 2, 7, 26, 94, 332, 1159, 4034, 14074, 49364, 174310. Prove that $a_{20} = 19691312684$.

3****.** Show that the sequence from the previous exercise also satisfies a recurrence of order 3 and degree 1.

4****.** Prove that $\exp(x\sqrt{1+x}) + \frac{1}{\sqrt{1+x}}$ is D-finite by finding a differential equation which has this function among its solutions.

5★. Let $r, d \in \mathbb{N}$ and let $V_{r,d}$ denote the vector space computed by Algorithm 1.33 or 1.34. Show that $\dim_C V_{r,d+1} \geq 2\dim_C V_{r,d} - \dim_C V_{r,d-1}$ whenever $d \geq 1$, and that $\dim_C V_{r+1,d} \geq 2\dim_C V_{r,d} - \dim_C V_{r-1,d}$ whenever $r \geq 1$.

6. Let p_n denote the nth prime number, and let $p(x) = \sum_{n=1}^{\infty} p_n x^n$. Prove that $p(x)$ does not satisfy any linear differential equation of order at most 5 with polynomial coefficients of order at most 10.

7★. Determine $\dim V_{100}$ for $0 \leq r, d \leq 5$ for the sequence $a_n = n(n+1)(n+2)(n+3)$.

8. Guess a differential equation for the solution of the functional equation of Exercise 22 in Sect. 1.1, as well as a recurrence for its coefficient sequence.

9. For a fixed $n_0 \in \mathbb{N}$, consider the sequence $(a_n)_{n=0}^{\infty}$ defined by

$$a_n = \begin{cases} 0, & \text{if } n < n_0, \\ \frac{1}{(n-n_0)!}, & \text{if } n \geq n_0. \end{cases}$$

Show that $(a_n)_{n=0}^{\infty}$ satisfies a recurrence of order $r = 1$ with polynomial coefficients of degree $d = 1$. How many initial terms need to be known in order to find it?

10. Instead of guessing a linear relation with polynomial coefficients between a series f and its derivatives $f', f'', \ldots$ (viz. a differential equation), we may use an analogous technique to find linear relations with polynomial coefficients between a series f and its powers $f^2, f^3, \ldots$ (viz. an algebraic equation). In this way, guess the minimal polynomial of the algebraic function $f(x) = (1-x)^{1/2} + (1-x^2)^{-1/3}$.

11. More generally, guessing can also be used to find linear relations with polynomial coefficients among several given sequences or power series. Use this to find a representation of $\sum_{k=1}^{n} \left(\sum_{i=1}^{k} \frac{1}{i}\right)^2$ as a quadratic polynomial in $\sum_{k=1}^{n} \frac{1}{k}$ with coefficients that are polynomials in n.

12. Guessing can also be used to find equations for multivariate series or sequences. Use this to find a bivariate recurrence for the sequence $(a_{n,m})_{n,m=0}^{\infty}$ where $a_{n,m} = \sum_{k=0}^{n} \binom{m}{k}^2$.

13. There is an infinite sequence $(a_n)_{n=0}^{\infty}$ in $\mathbb{Z}$ whose first terms modulo 59 are $1, 2, 6, 20, 11, 16$. Make a guess for the value a_5.

14★. Show that the sequence $(a_n)_{n=0}^{\infty}$ with $a_n = 5^{n^3}$ is D-finite when viewed as sequence in $\mathbb{Z}_p$, for any prime p, but it is not D-finite when viewed as sequence in $\mathbb{Z}$.

15. For sequences or power series over $\mathbb{Q}(t)$ involving a parameter t, we can use homomorphic images to get rid of the parameter and also to shorten the rational numbers to elements of a finite field. This can be done in two ways, either $\mathbb{Q}(t) \xrightarrow{eval} \mathbb{Q} \xrightarrow{mod} \mathbb{Z}_p$ or $\mathbb{Q}(t) \xrightarrow{mod} \mathbb{Z}_p(t) \xrightarrow{eval} \mathbb{Z}_p$. Which of them is better?

16. The boundary of the gray region of the figure in Example 1.36 is typically described by a hyperbola. There are constants α, β, γ such that there exists an equation of order r and degree d if and only if $r > \gamma$ and $d \geq \alpha + \frac{\beta}{r-\gamma}$. How would you implement step 7 of Algorithm 1.40 if α, β, γ are known?

17*. (Christoph Koutschan) Here is another trick that sometimes allows to reduce the number of primes. Consider the sequence $(a_n)_{n=0}^{\infty}$ with $a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k}^4$. There are polynomials $p_0, \ldots, p_6 \in \mathbb{Z}[x]$ of degree 18 such that $p_0(n)a_n + \cdots + p_6(n)a_{n+6} = 0$. Find them and compare the longest integer coefficient appearing in any of the polynomials $p_0(x), \ldots, p_6(x)$ to the longest integer coefficient appearing in any of the polynomials $p_0(x-3), p_1(x-3), \ldots, p_6(x-3)$.

18. Use Algorithm 1.40 to conjecture a recurrence for the sequence $(a_n)_{n=0}^{\infty}$ defined by $a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2n+k}{k} \binom{n+2k}{k}$.

19. Use Algorithm 1.40 to conjecture a differential equation for $a(x) = \sum_{n=0}^{\infty} a_n x^n$ where a_n is as in the previous exercise.

20*. A series $f \in C[[x]]$ is called *even* if $f(x) = f(-x)$, i.e., if $[x^n]f = 0$ for every odd integer n. It is called *odd* if $f(x) = -f(-x)$, i.e., if $[x^n]f = 0$ for every even integer n. How can we exploit the knowledge that a series is even for guessing a differential equation?

References

Obviously, the idea of guessing a pattern in an infinite sequence from a given finite number of terms is very old. So is the idea of employing the computer for this task. Rubey and Hebisch [233] trace the history back to a program written in 1964 by Pivar and Finkelstein [358]. In the 1990s, several implementations of a variety of different techniques for guessing appeared, including software by Bergeron and Plouffe [55] trying to express a given truncated series as some transformation of a rational series, software by Brak and Guttmann [107] for fitting data to algebraic or D-finite functions in order to estimate the asymptotic behavior, software by Krattenthaler [298] to express a given sequence as an iterated product over a rational function, software by Salvy and Zimmermann [379] and by Mallinger [319] for guessing D-finite recurrences and differential equations. Further implementations are available in the software packages mentioned at the end of Sect. 1.4.

There are some additional ways by which a guessed equation can be tested for plausibility. For any given prime p, one can associate to a differential equation a certain matrix called the p-curvature. For meaningful equations, this matrix tends to be nilpotent, while for wrong guesses it has very low chances to be nilpotent. See [75] for a more detailed discussion.

The idea of trading order for degree appears in [71, 76, 103]. See Sect. 4.2 for an explanation of this phenomenon.

With the computation in Example 1.32, we can only prove for any fixed r and d that the sequence of primes does not satisfy any recurrence of order r and degree d. It is more difficult to show that this sequence does not satisfy any such recurrence, regardless of the choice of r and d. A proof of this stronger fact was given by Flajolet, Gerhold, and Salvy [196].

A completely different approach to guessing is pursued by Sloane [410], who maintains a large database of known integer sequences. If the first few terms of an integer sequence are known, the database can be queried for known sequences starting with these terms.

1.6 Hermite-Padé Approximation

An approximation to a function f is a function g which in a certain sense is close to f. For sufficiently well-behaved functions, Taylor polynomials are good approximations in a neighborhood of the expansion point. These are the polynomials obtained by truncating the series expansion at some order. For example, $1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3$ is the fourth Taylor polynomial for the exponential function. We can also approximate a function by a rational function instead of a polynomial. If we choose a rational function whose expansion at 0 agrees with the series expansion of the function to be approximated, the approximation quality near the expansion point will not be worse than the quality of the Taylor polynomial, and it may be better than the Taylor polynomial at some distance from the expansion point.

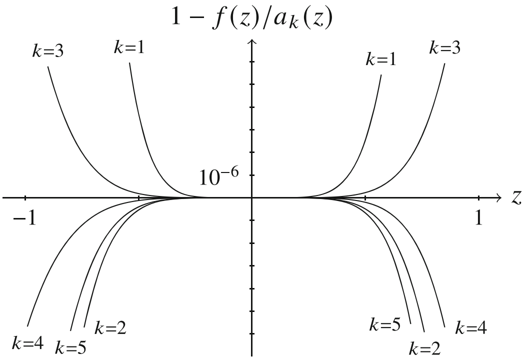
The construction of rational functions whose expansion at 0 matches a prescribed polynomial is a special case of the rational reconstruction problem of part 6 of Theorem 1.21. Given $a \in C[x]$ of degree $\leq n$ and some $k \in \{0, \dots, n\}$, the task consists of finding polynomials $p, q \in C[x]$ with $\deg(p) < k$ and $\deg(q) \leq n - k$ such that $p \equiv aq \bmod x^n$. If a is the nth Taylor polynomial of an analytic function, the resulting rational functions p/q are called *Padé approximants.*

Example 1.41 Consider the function $f : \mathbb{R} \to \mathbb{R}$ with $f(0) = 1$ and $f(z) = \frac{z}{e^z - 1}$ for $z \neq 0$. Its sixth Taylor polynomial is $1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4$. This polynomial translates into the following Padé approximants:

$$\begin{aligned}
k = 6 \text{ and } k = 5: &\quad a_5 = 1 - \tfrac{1}{2}x + \tfrac{1}{12}x^2 - \tfrac{1}{720}x^4 \\
k = 4: &\quad a_4 = \frac{-x^3 + 12x^2 - 60x + 120}{2(x^2 + 60)} \\
k = 3: &\quad a_3 = \frac{12(x^2 - 10x + 30)}{x^3 + 12x^2 + 60x + 360} \\
k = 2: &\quad a_2 = -\frac{120(x - 6)}{x^4 + 10x^3 + 60x^2 + 240x + 720}
\end{aligned}$$

$$k = 1: \quad a_1 = \frac{720}{x^5 + 6x^4 + 30x^3 + 120x^2 + 360x + 720}$$

The accuracy of all of these approximations is so good that it is hard to see a difference in the plots. It is more instructive to plot how much $f(z)/a_k(z)$ deviates from 1 as z varies. The lower the deviation, the better the approximation.



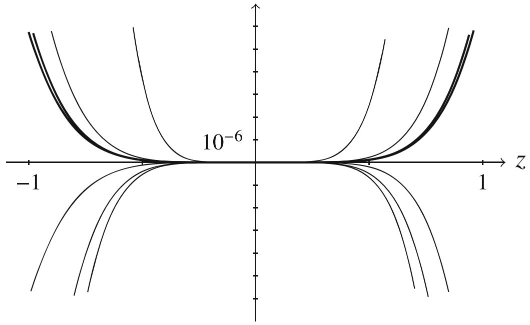
The best choice appears to be $k = 4$. □

If rational functions have a chance to approximate functions better than plain polynomials, why stop there? We could hope to get even better approximations by using D-finite functions instead of rational functions. The question is thus how to find for a given $a \in C[x]$ of degree N a D-finite function satisfying a differential equation equation of some prescribed order r with polynomial coefficients of some prescribed degree d such that its Nth Taylor polynomial agrees with a. Such D-finite functions are also known as *differential approximants.* One way to find a differential approximant is to apply the linear algebra approach previously discussed in the context of guessing, but with r and d chosen in such a way that the linear system becomes underdetermined rather than overdetermined. This way, we are guaranteed to find some solutions, and while there is no longer any confidence whatsoever that the function under consideration may actually be a solution of the equations we find, we can at least be sure that every equation obtained in this way has a solution whose Nth Taylor polynomial is a. We can use these functions as approximations.

Example 1.42 Continuing the previous example, consider again the truncated series $1 - \frac{1}{2}x + \frac{1}{12}x^2 + 0x^3 - \frac{1}{720}x^4 + 0x^5 + \mathrm{O}(x^6)$. Apply the methods of the previous section to search for potential differential equations of order 2 and degree 1. This leads to a linear system with six unknowns and four equations. Its solution space is generated by two vectors that correspond to the differential equations

$$7g(x) - (5x - 9)g'(x) - 3(x + 5)g''(x) = 0,$$
$$7xg(x) + 3(13x + 20)g'(x) + 15(x + 12)g''(x) = 0.$$

Each of these equations has a unique solution of the form $g(x) = 1 - \frac{1}{2}x + \frac{1}{12}x^2 + \cdots \in C[[x]]$. Interpreting the formal power series as analytic functions, we can compare the plots of $1 - f(z)/g(z)$ for each of these two series g to the corresponding plots for the Padé approximants. As we can see from the figure below, both D-finite approximants (shown in bold) yield better approximations than all of the Padé approximants that can be constructed from the same amount of data.



□

We can also use differential approximants to estimate the next term(s) in a formal power series.

Example 1.43 Let $f = \frac{x}{\exp(x)-1} \in C[[x]]$, and let $g_1, g_2 \in C[[x]]$ be the formal power series solutions of the two differential equations stated in the previous example whose first five terms match those of f. We have $[x^6]f = \frac{1}{30240}$ and $[x^6]g_1 = [x^6]g_2 = \frac{13}{324000}$. The error is about 20%, which is perhaps not too impressive.

It works better if we have more data. Assuming instead that we know the first 34 terms of the series f, we can construct a differential equation of order 2 with polynomial coefficients of degree 10 (notice $(2+1)(10+1) = 33 < 34$). If g is the unique power series solution of this equation whose first 34 terms match those of f, then the next few terms of g are pretty close to the corresponding terms of f:

$$\frac{[x^{36}]f}{[x^{36}]g} \approx 1.0000000000000000001028,$$

$$\frac{[x^{38}]f}{[x^{38}]g} \approx 0.9999999999999999990456,$$

$$\frac{[x^{40}]f}{[x^{40}]g} \approx 0.9999999999999999961510,$$

$$\frac{[x^{42}]f}{[x^{42}]g} \approx 0.9999999999999999907264,$$

$$\frac{[x^{44}]f}{[x^{44}]g} \approx 0.99999999999999999822612,$$

$$\frac{[x^{46}]f}{[x^{46}]g} \approx 0.99999999999999999704010,$$

$$\frac{[x^{48}]f}{[x^{48}]g} \approx 0.99999999999999999549103,$$

$$\frac{[x^{50}]f}{[x^{50}]g} \approx 0.99999999999999999356414.$$

□

We can construct differential approximants with essentially the same techniques used in the previous section for guessing. There is also another approach which can be used for computing differential approximants or for guessing, which we will discuss next. The techniques discussed earlier take advantage of the fact that the set of differential equations satisfied by a D-finite function forms a vector space over the constant field C. Besides multiplication by a constant, also multiplication by a polynomial turns a correct equation into another correct equation, so the set of correct equations even forms a $C[x]$-module. For a fixed order r and a given number N of terms, we can consider the $C[x]$-module consisting of all equations of order r (and arbitrary degree d) matching the first N terms. This module has infinite dimension as a C-vector space but is finitely generated as a $C[x]$-module, so we can ask for a $C[x]$-module basis.

Suppose there are r formal power series $f_1, \dots, f_r$ for which we know the coefficients of $x^0, \dots, x^{N-1}$. The task is then to determine all of the polynomial vectors $(p_1, \dots, p_r) \in C[x]^r$ such that $x^N \mid p_1 f_1 + \cdots + p_r f_r$. There are always trivial solutions such as $(x^N, 0, \dots, 0)$, which are usually not interesting because they don't tell us anything about the series f_i but are rather a side effect of the truncation. The interesting relations are those which consist of polynomials whose degrees are small compared to N. Our goal is therefore to find a basis of the solution space in which the degrees of the basis vectors are, in a sense, as small as possible. We can then expect that "true" relations, if there are any, show up in such a basis as soon as N is large enough.

We say that the degrees of the basis vectors $b_1, \dots, b_r$ are as small as possible if every solution $(p_1, \dots, p_r)$ of degree at most d can be written as a linear combination $q_1 b_1 + \cdots + q_r b_r$ with $\deg q_i + \deg b_i \le d$ for all i. Note that this is not true in general, because monomials contributed by some of the summands $q_i b_i$ may cancel each other so that the resulting linear combination has lower degree. The precise definition is as follows. We state it for a slightly generalized notion of degree that allows us to add some penalties δ_i to the coordinate degrees. This will become handy later. A user will typically want to choose $\delta = (0, \dots, 0)$.

Definition 1.44 Let $f = (f_1, \dots, f_r) \in C[[x]]^r$ be a vector of formal power series, let $\delta = (\delta_1, \dots, \delta_r) \in \mathbb{N}^r$ be a vector of natural numbers, and let $\sigma \in \mathbb{N}$.

1. The *relative degree* of $p = (p_1, \dots, p_r) \in C[x]^r$ with respect to δ is defined as $\deg^\delta p := \max\{\delta_i + \deg p_i : i = 1, \dots, r\}$. (Convention: $\deg 0 := -\infty$.)
2. The *order* $\operatorname{ord}_f p$ of $p = (p_1, \dots, p_r) \in C[x]^r$ with respect to f is defined as the largest $N \in \mathbb{N} \cup \{\infty\}$ such that $x^N \mid p_1 f_1 + \cdots + p_r f_r$.
3. For $d \in \mathbb{N} \cup \{\infty\}$, define $M_{\sigma,d} := \{\, p \in C[x]^r : \deg^\delta p \leq d, \operatorname{ord}_f p \geq \sigma \,\}$. (The dependence of $M_{\sigma,d}$ on f and δ is not reflected in the notation.)
4. A set $\{b_1, \dots, b_r\} \subseteq C[x]^r$ is called a *σ-basis* for f with respect to δ if $\operatorname{ord}_f b_i \geq \sigma$ for all $i = 1, \dots, r$ and if for every $d \in \mathbb{N} \cup \{\infty\}$ and every $p \in M_{\sigma,d}$ there exists a unique vector $(q_1, \dots, q_r) \in C[x]^r$ with $\deg q_i + \deg^\delta b_i \leq d$ $(i = 1, \dots, r)$ and $p = q_1 b_1 + \cdots + q_r b_r$. □

The idea behind the following algorithm is simple. In each iteration, it checks which basis vectors violate the current order constraint. Among these, it chooses one of least degree and adds suitable constant multiples of it to the other basis elements, so as to increase their order. This leaves the chosen basis vector as the only one that violates the order condition. This violation is then cured by multiplying this vector by x.

Algorithm 1.45
Input: *A number $\sigma \in \mathbb{N}$. A vector $f = (f_1, \dots, f_r) \in C[[x]]^r$, where for each coordinate f_i (at least) the coefficients of $x^0, \dots, x^{\sigma-1}$ are known. A vector $\delta = (\delta_1, \dots, \delta_r) \in \mathbb{N}^r$.*
Output: *A matrix $B \in C[x]^{r \times r}$ whose columns form a σ-basis for f with respect to δ. These are referred to as the Hermite-Padé approximants of f.*

1 *for $i = 1, \dots, r$ do*
2   *Set b_i to the ith unit vector of $C[x]^r$.*
3 *for $s = 0, \dots, \sigma - 1$ do*
4   *for $i = 1, \dots, r$ do*
5   *Let $c_i := [x^s]\big(b_i \cdot f\big)$.*
6   *Let $L = \{\ell : c_\ell \neq 0\}$.*
7   *if $L \neq \emptyset$ then*
8   *Choose some $\ell \in L$ for which $\deg^\delta b_\ell$ is minimal.*
9   *for $i \in L \setminus \{\ell\}$ do*
10   *Set $b_i = b_i - \frac{c_i}{c_\ell} b_\ell$.*
11   *Set $b_\ell = x\, b_\ell$.*
12 *Return $B = (b_1, \dots, b_r) \in C[x]^{r \times r}$.*

Theorem 1.46 *Algorithm 1.45 is correct.* □

Proof We show by induction on s that $\{b_1, \dots, b_r\}$ is a σ-basis for $\sigma = s$ right before line 4.

This is true for $s = 0$, because in this case $x^0 \mid p_1 f_1 + \cdots + p_r f_r$ is true for all $p_1, \dots, p_r \in C[x]$, so $M_{0,d} = \{\, p \in C[x]^r : \deg^\delta p \leq d \,\}$, and for every

$d \in \mathbb{N} \cup \{\infty\}$ and every $p \in M_{0,d}$ there is a unique representation of p as a linear combination of unit vectors with coefficients whose degrees do not exceed d.

Now let $s \in \{0, \ldots, \sigma - 1\}$ be arbitrary. Write $b_1, \ldots, b_r$ for the values of the b_i right before line 4, and $b'_1, \ldots, b'_r$ be the values of the b_i right after line 11. Assume as the induction hypothesis that $\{b_1, \ldots, b_r\}$ is a σ-basis for $\sigma = s$. We show that $\{b'_1, \ldots, b'_r\}$ is a σ-basis for $\sigma = s + 1$. If $L = \emptyset$, then $M_{s+1,d} = M_{s,d}$ and there is nothing to show. Consider the case if $L \neq \emptyset$.

First, since $\operatorname{ord}_f b_i \geq s$ for all i, the instructions in lines 10 and 11 ensure that $\operatorname{ord}_f b'_i \geq s + 1$ for all i.

Next, let $d \in \mathbb{N} \cup \{\infty\}$ and $p \in M_{s+1,d}$. Since $M_{s+1,d} \subseteq M_{s,d}$, there exists a unique vector $(q_1, \ldots, q_r) \in C[x]^r$ with $\deg q_i + \deg^\delta b_i \leq d$ $(i = 1, \ldots, r)$ and $p = q_1 b_1 + \cdots + q_r b_r$.

Because of line 8, we have $\deg^\delta b'_i \leq \deg^\delta b_i$ for $i \neq \ell$ and $\deg^\delta b'_\ell = 1 + \deg^\delta b_\ell$. Set $q'_i := q_i$ for $i \neq \ell$ and $q'_\ell := \frac{1}{x c_\ell}(c_1 q_1 + \cdots + c_r q_r)$. Then q'_ℓ is a polynomial, because $\operatorname{ord}_f p \geq s + 1$ implies that $[x^s]\big((q_1 b_1 + \cdots + q_r b_r) \cdot f\big) = [x^0](q_1 c_1 + \cdots + q_r c_r) = 0$.

We have $\deg q'_i = \deg q_i$ for $i \neq \ell$ and $\deg q'_\ell \leq d - \deg^\delta b_\ell - 1$, because $\deg^\delta b_i \geq \deg^\delta b_\ell$ for all i by line 8. So for all i we have $\deg q_i + \deg^\delta b_i \leq d$ for all i. A direct calculation also confirms that $p = q'_1 b'_1 + \cdots + q'_r b'_r$.

This shows the existence of a vector $(q'_1, \ldots, q'_r)$ with the required properties. To see that the vector is unique, observe that $(b'_1, \ldots, b'_r)$ is obtained from $(b_1, \ldots, b_r)$ through multiplication by a certain matrix $T \in C[x]^{r \times r}$ with nonzero determinant. Therefore, $(b'_1, \ldots, b'_r)$ is a product of several such matrices and is therefore invertible as a matrix over $C(x)$. In particular, $b'_1, \ldots, b'_r$ are linearly independent over $C[x]$. If $(\bar{q}'_1, \ldots, \bar{q}'_r)$ is another vector with the required properties, then $(\bar{q}'_1 - \bar{q}_1) b'_1 + \cdots + (\bar{q}'_r - \bar{q}_r) b'_r = 0$, so $\bar{q}'_i = \bar{q}_i$ for all i. ■

Theorem 1.47 *Algorithm 1.45 performs at most* $4r^2\sigma + 2r\sigma(\sigma - 1)$ *operations in* C. □

Proof All arithmetic operations take place in lines 5 and 10 (the multiplication in line 11 is only a shift of the coefficient array). We write $b_{i,j}$ for the jth coordinate of the vector b_i.

In line 5, the computation of a single c_i via

$$c_i = [x^s](b_i \cdot f) = \sum_{j=1}^{r} \sum_{u=0}^{\deg b_{i,j}} ([x^u] b_{i,j})([x^{s-u}] f_j)$$

requires at most $2 \sum_{j=1}^r (\deg b_{i,j} + 1)$ many additions and multiplications. The whole loop then takes at most $2 \sum_{i=1}^r \sum_{j=1}^r (\deg b_{i,j} + 1)$ operations. In each iteration of the outer loop, the degree of at most one vector b_i is incremented (in line 11; line 10 does not affect the degrees of the other vectors by the choice made in line 8), so we have $\sum_{i=1}^r \deg b_{i,j} \leq s$ for every j. The total number of operations in lines 4 and 5 is therefore bounded by $2r(s + r)$.

In line 10, we need to update at most $1 + \deg b_\ell$ coefficients in each of the r coordinates of each b_i. If we precompute $\frac{1}{c_\ell} b_\ell$ at the cost of $r(1 + \deg b_\ell)$ divisions before line 10, then line 10 requires at most $2r(|L| - 1)(1 + \deg b_\ell)$ multiplications and subtractions. In total, we get $2r|L|(1 + \deg b_\ell)$ operations. By the minimality of $\deg b_\ell$ we have $\sum_{i=1}^{r} \deg b_i \geq |L| \deg b_\ell$, which together with $\sum_{i=1}^{r} \deg b_i \leq s$ implies $\deg b_\ell \leq s/|L|$. Therefore, the total number of operations performed in lines 9 and 10 is bounded by $2r|L| + 2rs \leq 2r(s + r)$.

The bound in the theorem now follows via $\sum_{s=0}^{\sigma-1} 4r(s+r) = 4r^2\sigma + 2r\sigma(\sigma - 1)$. ■

In order to search for differential equations possibly satisfied by a formal power series $f \in C[[x]]$ in which the first N terms are known, apply Algorithm 1.45 with $f, f', \ldots, f^{(r)}$ as $f_1, \ldots, f_{r+1}$ and $\sigma = N - r$. It will always return a list of $r + 1$ vectors $p = (p_0, \ldots, p_r) \in C[x]^{r+1}$ for which we have $x^{N-r} \mid p_0 f + \cdots + p_r f^{(r)}$. If some of the vectors in the output have coordinates of lower degree than the others, then this gives some evidence that we may actually have $p_0 f + \cdots + p_r f^{(r)} = 0$. If not, we can still use the elements of the basis to define differential approximants.

Example 1.48 Let $f(x) = x^3 + (1-2x)\exp(x)$. We want to find a potential relation among f, f', f''. After step 1 of the algorithm, we have

$$\begin{aligned} b_1 &= (1, 0, 0), & b_1 \cdot (f, f', f'') &= 1 + \mathrm{O}(x) \\ b_2 &= (0, 1, 0), & b_2 \cdot (f, f', f'') &= -1 + \mathrm{O}(x) \\ b_3 &= (0, 0, 1), & b_3 \cdot (f, f', f'') &= -3 + \mathrm{O}(x). \end{aligned}$$

So all of the b_i's have order and degree zero. In the following table we show the degrees and orders of the b_i at the beginning of each loop iteration.

σ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\deg b_1$	0	1	1	1	2	2	2	3	3	3	4	4	5	5	6	6
$\deg b_2$	0	0	1	1	1	2	2	2	3	3	3	4	4	5	5	6
$\deg b_3$	0	0	0	1	1	1	2	2	2	3	3	3	3	3	3	3
$\operatorname{ord} b_1$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\operatorname{ord} b_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\operatorname{ord} b_3$	0	1	2	3	4	5	6	7	8	9	10	>16	>16	>16	>16	>16

This is a typical run of the algorithm. We see that the adjustments of the basis vectors are made in such a way that the orders are always at least σ in each iteration, and at most one basis vector per iteration increases its degree. The order increases usually by one only. At iteration $\sigma = 11$, the order of b_3 makes a bigger leap. In fact, it grows beyond what is measurable by the available number of terms. From this point on, the vector b_3 does not change. The output basis thus has two vectors of degree 6, which are of no use, and one vector of degree 3, which corresponds to an actual relation between f, f', f''. □

Typically the degrees of the polynomial coefficients in a differential equation are larger than the order of the equation. For example, we may have $d \approx r^2$. In such situations, we need about $N \approx r^3$ terms to recover the equation. Algorithm 1.45 will take roughly $4r^2r^3 + 2rr^6 \approx r^7$ operations while Algorithm 1.34 will take $(r^3)^3 \approx r^9$ steps if classical Gaussian elimination is used for solving the linear system. If fast matrix multiplication is exploited, it will still take $r^{3\omega}$ steps, so in order to beat Algorithm 1.45 we would need $\omega \leq 2.33$, which is feasible in theory but not in practice.

So Algorithm 1.45 is superior to the linear algebra approach. But we can still do better. A deficiency of Algorithm 1.45 is that in line 10 it multiplies a field element to a polynomial. Instead of many such multiplications of a low-degree polynomial by a high-degree polynomial, it would be better to have a smaller number of multiplications of two high-degree polynomials, so that the algorithm can take advantage of fast multiplication algorithms.

Such an algorithm can be obtained from the following theorem, which allows us to break the problem into two pieces of the same type but half the size. The algorithm solves the two problem parts recursively, and the combination of the two partial solutions involves the desired balanced multiplications.

Theorem 1.49 *Suppose Algorithm 1.45 is implemented in such a way that in line 8 it always chooses the smallest eligible ℓ. Let $f = (f_1, \ldots, f_r) \in C[[x]]^r$, $\sigma, \sigma' \in \mathbb{N}$, and $\delta = (\delta_1, \ldots, \delta_r) \in \mathbb{N}^r$.*

Let $B = (b_1, \ldots, b_r) \in C[x]^{r\times r}$ be the σ-basis for f with respect to δ computed by Algorithm 1.45. Let $B'' \in C[x]^{r\times r}$ be the $(\sigma + \sigma')$-basis for f with respect to δ computed by Algorithm 1.45.

Let $(f_1', \ldots, f_r')^T = x^{-\sigma} B\,(f_1, \ldots, f_r)^T$, $\delta' = (\deg^{\delta} b_1, \ldots, \deg^{\delta} b_r) \in \mathbb{N}^r$, and let $B' \in C[x]^{r\times r}$ be the σ'-basis for $(f_1', \ldots, f_r')$ with respect to δ' computed by Algorithm 1.45.

Then $B'' = B'B$. □

Proof In every iteration of Algorithm 1.45, the matrix B is updated to $T_s B$ for some matrix $T_s \in C[x]^{r\times r}$. In the end, we have $B = T_{\sigma-1} \cdots T_0$ and $B'' = T_{\sigma+\sigma'-1} \cdots T_0$, respectively. To prove the theorem, we show that $B' = T_{\sigma+\sigma'-1} \cdots T_\sigma$.

We show by induction on s that the transformation matrix $T_{\sigma+s}$ in the computation of B'' agrees with the transformation matrix T_s' in the computation of B'. For $s = 0$ there is nothing to show. Assume it is true for some s.

Then in the sth iteration of the computation of B' we have $(c_1, \ldots, c_r)^T = [x^s](B' \cdot f') = [x^s](B' \cdot x^{-\sigma} B\, f) = [x^{s+\sigma}](T_{\sigma+s-1} \cdots T_\sigma \cdot T_{\sigma-1} \cdots T_0 \cdot f)$, which by the induction hypothesis agrees with the value of c_i in the $(s + \sigma)$th iteration of the computation of B''.

If we write $b_i' = (b_{i,1}', \ldots, b_{i,r}')$ and likewise for b_i and b_i'', then

$$\deg^{\delta'} b_i' = \max_{j=1}^{r}(\delta_j' + \deg b_{i,j}')$$

$$
\begin{aligned}
&= \max_{j=1}^{r}(\deg^{\delta} b_j + \deg b'_{i,j}) \\
&= \max_{j=1}^{r}(\max_{k=1}^{r}(\delta_k + \deg b_{j,k}) + \deg b'_{i,j}) \\
&= \max_{k=1}^{r}(\delta_k + \max_{j=1}^{r}(\deg b'_{i,j} + \deg b_{j,k})) \\
&\geq \max_{k=1}^{r}(\delta_k + \deg b''_{i,k}) = \deg^{\delta} b''_i .
\end{aligned}
$$

The only way how we could have $\deg^{\delta} b''_i < \deg^{\delta'} b'_i$ for some i is if there is a degree drop in line 10 at some iteration in the computation of B''. Such degree drops are impossible because B'' is a σ-basis for $\sigma = s$ at the beginning of the sth iteration, and a degree drop would give rise to a violation of the minimality condition in the definition of σ-basis.

Therefore we actually have $\deg^{\delta} b''_i = \deg^{\delta'} b'_i$, so the set L in the sth iteration of the computation of B' agrees with the set L in the $(s + \sigma)$th iteration of the computation of B''. Since L and the c_i agree and we assume that the choice in line 8 is made in a canonical way, it follows that $T_s = T'_s$, as claimed. ■

Algorithm 1.50
Input and Output like for Algorithm 1.45.

1 *If σ is smaller than some suitably chosen constant, call Algorithm 1.45 and return the result.*
2 *Set $\tilde{\sigma} = \lfloor \sigma/2 \rfloor$.*
3 *Call Algorithm 1.50 recursively with $\tilde{\sigma}$ as σ, $f \bmod x^{\tilde{\sigma}}$ as f, and δ as δ. Let $B = (b_1, \ldots, b_r)$ be the result.*
4 *Set $(f')^T = (x^{-\tilde{\sigma}} B f^T) \bmod x^{\sigma-\tilde{\sigma}}$ and $\delta' = (\deg^{\delta} b_1, \ldots, \deg^{\delta} b_r)$.*
5 *Call Algorithm 1.50 recursively with $\sigma - \tilde{\sigma}$ as σ, f' as f, and δ' as δ. Let B' be the result.*
6 *Return $B'B$.*

Theorem 1.51 *Algorithm 1.50 is correct and requires at most* $\mathrm{O}(r\mathrm{M}(r\sigma)\log\sigma)$ *operations in C.* □

Proof The correctness follows directly from Theorem 1.49.

The main contributions to the cost of the algorithm are the two recursive calls in lines 3 and 5 and the computation of Bf^T in line 4 and of $B'B$ in line 6. For simplicity, and without loss of generality, let us assume σ is a power of two.

Line 4 is a multiplication of an $r \times r$ matrix to a vector of length r, where matrix and vector contain polynomials of degree at most $\sigma/2$. This multiplication can be carried out using $\mathrm{O}(r^2\mathrm{M}(\sigma))$ operations in C.

Line 6 is the multiplication of two $r \times r$ matrices B' and B with polynomial entries of degree at most $\sigma/2$. This can be done using $\mathrm{O}(r^3\mathrm{M}(\sigma))$ operations in C. In order to get a better bound, let $d'_1, \ldots, d'_r$ denote the degrees of the columns of B'

and let $d_1, \ldots, d_r$ be the degrees of the columns of B. Then we have $\sum_{i=1}^r d_i' \le \sigma/2$ and $\sum_{i=1}^r d_i \le \sigma/2$, because Algorithm 1.45 increments the degree of at most one basis element in each iteration. Therefore, the multiplications in the matrix product $B'B$ actually cost only

$$\begin{aligned}\sum_{i=1}^r\sum_{j=1}^r\sum_{k=1}^r \mathrm{M}(\max(d_k', d_j)) &\le \sum_{i=1}^r\sum_{j=1}^r\sum_{k=1}^r \mathrm{M}(d_k' + d_j)\\ &\le \sum_{i=1}^r \mathrm{M}\Big(\sum_{j=1}^r\sum_{k=1}^r (d_k' + d_j)\Big) \le r\mathrm{M}\Big(r\sum_{j=1}^r d_j + r\sum_{k=1}^r d_k'\Big) \le r\mathrm{M}(r\sigma)\end{aligned}$$

operations. The cost of the additions is bounded by $\mathrm{O}(r^2\sigma)$ using a similar argument.

In summary, we have that lines 4 and 6 require at most $\mathrm{O}(r\mathrm{M}(r\sigma))$ many additions and multiplications in C, say at most $\alpha r\mathrm{M}(r\sigma)$ for some constant $\alpha > 0$. For the total number $T(\sigma)$ of operations required by Algorithm 1.50 we then have

$$T(\sigma) \le 2T(\sigma/2) + \alpha r\mathrm{M}(r\sigma).$$

It can now be checked inductively that $T(\sigma) \le \beta r\mathrm{M}(r\sigma)\log\sigma$ for some constant $\beta > 0$. ■

Example 1.52 Consider again the series $f \in \mathbb{Q}[[x]]$ from Example 1.48. If we call Algorithm 1.45 with $\sigma = 8$ and $\delta = (0, 0, 0)$ on (f, f', f''), the result is a basis $B = (b_1, b_2, b_3)$ with $\deg b_1 = 3$, $\deg b_2 = 3$, $\deg b_3 = 2$ and $\operatorname{ord} b_1 = \operatorname{ord} b_2 = \operatorname{ord} b_3 = 8$.

Next call Algorithm 1.45 with $\sigma = 8$ and $\delta = (3, 3, 2)$ on $x^{-8}B \cdot (f, f', f'')^T$. The result is a basis $B' = (b_1', b_2', b_3')$ with $\deg^\delta b_1' = 6$, $\deg^\delta b_2' = 6$, $\deg^\delta b_3' = 3$ and $\operatorname{ord} b_1' = \operatorname{ord} b_2' = 7$, $\operatorname{ord} b_3' > 8$.

For the product $B'B$ we get the same result as before. □

For the typical situation where we want to reconstruct an equation of order r and degree $d \approx r^2$ from $\sigma \approx r^3$ terms, the number of operations of Algorithm 1.50 is bounded by $r\mathrm{M}(r^4)\log(r^3) \approx r^5\log(r)^2$. This is considerably better than the bound $\approx r^7$ obtained for Algorithm 1.45, and much better than the bound $\approx r^9$ obtained for Algorithm 1.34.

Exercises

1. The function arcsin is D-finite but not algebraic. Construct an approximating algebraic function with a minimal polynomial $p(x, y)$ with degrees $\deg_x p = 3$ and $\deg_y p = 2$ from the truncation $\arcsin(x) = x + \frac{1}{6}x^3 + \frac{3}{40}x^5 + \frac{5}{112}x^7 + \frac{35}{1152}x^9 +$

$\mathrm{O}(x^{11})$. Compare the accuracy of the approximation at $x = 0.9$ to the accuracy of the Padé approximants obtained from these terms.

2. The sequence $(a_n)_{n=0}^{\infty}$ with $a_n = n^n$ is not D-finite. Using the terms for $n = 0, \ldots, 15$, set up a recurrence of order two and degree four, and show that it correctly predicts the term a_{16} in the sense that the actual value a_{16} is the nearest integer to the rational number produced by the recurrence.

3*. Let $f \in C[[x]]^r$, $\delta \in \mathbb{N}^r$ and $d, \sigma \in \mathbb{N}$. Suppose that $\{b_1, \ldots, b_r\} \subseteq C[x]^r$ is a σ-basis for f with respect to δ. Show that $M_{\sigma,d}$ is generated as a C-vector space by $\{x^i b_j : j = 1, \ldots, r, i = 0, \ldots, d - \deg^{\delta} b_j\}$.

4. The series $1/(1 - x + 2x^2)\exp(x\sqrt{1-x}) \in C[[x]]$ satisfies a linear differential equation of order two with polynomial coefficients of degree five. Use Algorithm 1.45 to find it.

5. The series $\frac{x^3+1}{1-x}\exp(x)$ satisfies two distinct (i.e., C-linearly independent) linear differential equations of order two with polynomial coefficients of degree at most three. Use Algorithm 1.45 to find them.

6. Are σ-bases uniquely determined by f, δ, and σ?

7. Implement Algorithm 1.45 and 1.50 in a computer algebra system that uses fast (i.e., subquadratic) polynomial multiplication. Experiment with different problem sizes in order to find a good choice for the bound on σ used in line 1 of Algorithm 1.50.

8.** Example 1.48 suggests that a basis vector b_i corresponds to a correct relation if its order is larger than the current value of s during the execution of Algorithm 1.45. But of course there is no guarantee. Construct an example where during the execution of Algorithm 1.45 the order of some b_i increases to $s + 5$, but continues to change later during the algorithm.

9. Let $B = (b_1, \ldots, b_r) \in C[x]^{r \times r}$ be a σ-basis. Show that $\det(B)$ is a power of x.

10*. Prove the complexity estimate of part 6 of Theorem 1.21.

11. Find a rational function p/q with $\deg p \leq 2$ and $\deg q \leq 6$ whose series expansion starts like $1+5x+4x^2+3x^3+7x^4+36x^5+84x^6+142x^7+231x^8+497x^9$.

12*. For a sequence $a = (a_n)_{n=0}^{\infty} \in C^{\mathbb{N}}$ that is not identically zero, define $\operatorname{ord} a$ as the smallest $N \in \mathbb{N}$ with $a_N = 0$ and $a_{N+1} \neq 0$. For the zero sequence, define $\operatorname{ord} 0 := +\infty$.

For a vector $f = (f_1, \ldots, f_r) \in (C^{\mathbb{N}})^r$ of sequences and a vector $p = (p_1, \ldots, p_r) \in C[x]^r$ of polynomials, define $\operatorname{ord}_f p := \operatorname{ord}(p_1 f_1 + \cdots + p_r f_r)$. With this meaning of order, σ-bases for vectors of sequences are defined literally as in part 4 of Definition 1.44.

Modify Algorithms 1.45 and 1.50 to handle this case.

References

Padé considered in his thesis [347] the problem of finding rational functions whose series expansion matches a prescribed truncated series. Only a year after Padé, Hermite [237] formulated the more general question discussed in this section: for given power series $f_1, \ldots, f_r \in C[[x]]$ find polynomials $p_1, \ldots, p_r \in C[x]$ of low degree such that $p_1 f_1 + \cdots + p_r f_r = \mathrm{O}(x^\sigma)$ for some large σ.

The efficient computation of Hermite-Padé approximants was studied by several authors. The algorithms presented here are due to Beckermann and Labahn [50]. Our discussion closely follows their paper. For earlier results, see [48, 49, 431] and the references given there.

The algorithms of Beckermann and Labahn actually solve a more general version of the problem. In their version, the algorithms take an additional parameter, $\rho \in \mathbb{N} \setminus \{0\}$, as input, and in line 8 of Algorithm 1.45 they set $b_\ell = x^\rho b_\ell$ instead of $b_\ell = x b_\ell$. This modification can be used for finding polynomial relations between vectors of power series, i.e., polynomials $p_1, \ldots, p_r \in C[x]$ such that for given $f_1 = (f_{1,1}, \ldots, f_{1,\rho}), \ldots, f_r = (f_{r,1}, \ldots, f_{r,\rho}) \in C[[x]]^\rho$ we have

$$p_1 f_1 + \cdots + p_r f_r = \big(\mathrm{O}(x^\sigma), \ldots, \mathrm{O}(x^\sigma)\big).$$

See [50] for a detailed discussion and several applications. This generalized version is also used in the algorithm of Storjohann and Villard [415] for efficient computation of nullspace bases of matrices with polynomial entries.

In the interest of simplicity, our proof of Theorem 1.51 assumes naive matrix multiplication. A version using fast matrix multiplication is given by Giorgi, Jeannerod and Villard [218].

Hermite-Padé approximation has been used for guessing in gfun and in software of Hebisch and Rubey [233]. Further applications in the context of D-finite functions are discussed in Chapter 10 of [73] and also in later sections of this book.

Chapter 2
The Recurrence Case in One Variable

2.1 Evaluation

A D-finite sequence is uniquely determined by a recurrence it satisfies and a suitable number of initial terms. Indeed, if the sequence $(a_n)_{n=0}^{\infty}$ satisfies the recurrence

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$$

for all $n \in \mathbb{N}$, then terms with sufficiently large indices can be computed from terms with lower indices by

$$a_n = -\frac{1}{p_r(n-r)}\big(p_0(n-r)a_{n-r} + \cdots + p_{r-1}(n-r)a_{n-1}\big).$$

The equation can be applied recursively until the specified initial values are reached.

The recursion is applicable to all indices n for which $p_r(n-r) \neq 0$. In the most simple case where $p_r(n-r) \neq 0$ is true for all $n \in \mathbb{N}$, it suffices to specify the terms $a_0, \ldots, a_{r-1}$ as initial values. If we have $p_r(n-r) = 0$ for some nonnegative integer n, then the value of a_n for such indices n does not follow from the earlier values. These terms must therefore be supplied as additional initial terms. All of the other terms can then be computed by repeatedly applying the recurrence, as follows:

Algorithm 2.1
Input: *A D-finite sequence* $(a_n)_{n=0}^{\infty}$ *specified by a recurrence equation* $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ *and initial values* $a_0, a_1, \ldots, a_{r-1}$, *as well as the terms* a_i *for every* $i \in \mathbb{N}$ *with* $p_r(i-r) = 0$; *an integer* $N \in \mathbb{N}$.
Output: *The term* a_N.

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1_2

1 *if* $N < r$, *then*
2   *Return* a_N *and stop.*
3 *Set* $(A_0, \ldots, A_{r-1}) = (a_0, a_1, \ldots, a_{r-1})$.
4 *for* $n = r, \ldots, N$ *do*
5   *if* $p_r(n-r) = 0$ *then*
6   *Set* $(A_0, \ldots, A_{r-1}) = (A_1, \ldots, A_{r-1}, a_n)$.
7   *else*
8   *Set* $(A_0, \ldots, A_{r-1}) = (A_1, \ldots, A_{r-1}, -\frac{1}{p_r(n-r)} \sum_{i=0}^{r-1} p_i(n-r)A_i)$.
9 *Return* A_{r-1}.

The correctness of the algorithm follows from the observation that at the end of each iteration of the main loop (i.e., right after line 8), the variable A_{r-1} contains the right value of a_n. This is easily proved by induction. Also the complexity of the algorithm is obvious: it requires $\mathrm{O}(rdN)$ arithmetic operations where d is the maximal degree of the polynomials p_i, and uses memory that does not grow with N.

Note that a naive recursive implementation leads to excessive recomputation: if the computation of a_n calls recursively the computation of a_{n-1} and a_{n-2}, their computations in turn call recursively the computation of a_{n-2}, a_{n-3} (initiated by a_{n-1}) and a_{n-3}, a_{n-4} (initiated by a_{n-2}) and so on, all the way down to the initial values. Thus, there is an exponential amount of recomputation which blows up the computation time to $\mathrm{O}(r^N d)$. This is not practical even for small examples. Some computer algebra systems allow to specify that functions should remember its outputs and return the cached value whenever it is called with previously called arguments. With this option, the computation time drops to $\mathrm{O}(rdN)$, but the memory requirement increases to $\mathrm{O}(N)$.

In order to compute several terms $a_{N_1}, a_{N_2}, \ldots, a_{N_k}$, Algorithm 2.1 should not be called several times. Instead, it should be exploited that during the computation of a term a_N, the algorithm encounters all of the previous terms, and it should be adapted to print out the desired terms along the way. In the extreme case where we need all terms $a_0, a_1, \ldots, a_N$ (for some finite given N), it is hard to imagine a significantly better method than Algorithm 2.1, for in this case, the output size and computation time essentially agree. Even if we take into account that the numbers get longer with increasing index, and that arithmetic operations are more costly for longer numbers, it is still reasonable to expect that the output size essentially agrees with the computation time. For example, if each a_n is an integer with $\approx \alpha n$ digits, for some constant α, then the total size of $a_1, \ldots, a_N$ is $\approx \frac{1}{2}\alpha N^2$. For the computation time, in the nth iteration of Algorithm 2.1, r numbers of length $\approx \alpha n$ (the previous terms $a_{n-1}, \ldots, a_{n-r}$) all get multiplied with numbers of size $\mathrm{O}(\log(n))$ (the coefficients of the recurrence), and the results are added up. This takes $\mathrm{O}(n \log(n))$ time, so the total time amounts to $\mathrm{O}^{\sim}(N^2)$ bit operations.

For computing a single isolated term, we may be able to do better. In order to explain how, we reformulate the recurrence as a matrix equation:

$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \\ \vdots \\ a_{n+r-1} \\ a_{n+r} \end{pmatrix} = \underbrace{\frac{1}{p_r(n)} \begin{pmatrix} 0 & p_r(n) & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & p_r(n) \\ -p_0(n) & -p_1(n) & \cdots & \cdots & -p_{r-1}(n) \end{pmatrix}}_{=:P(n)} \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+r-2} \\ a_{n+r-1} \end{pmatrix}.$$

If we assume for simplicity that p_r has no integer roots, then we have

$$\begin{pmatrix} a_{n-r+1} \\ \vdots \\ a_n \end{pmatrix} = P(n-r) \cdots P(1) P(0) \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix}$$

for all $n \in \mathbb{N}$. We can compute the value a_N for some specific index $N \in \mathbb{N}$ quickly if we can compute a matrix product $P(N-r) \cdots P(0)$ for some given polynomial matrix $P \in C[x]^{r \times r}$ quickly. In a sense, Algorithm 2.1 evaluates this matrix-product factor by factor:

$$\dots \underbrace{P(8)\; \underbrace{P(7)\; \underbrace{P(6)\; \underbrace{P(5)\; \underbrace{P(4)\; \underbrace{P(3)\; \underbrace{P(2) P(1)}}}}}}}.$$

At every step of the evaluation, this scheme multiplies a matrix $P(N)$ with relatively small entries with the product $P(N-1) \cdots P(0)$ of all previous factors, which typically contains much longer entries. The idea for the fast algorithm is to regroup the multiplications in such a way that matrices of similar size get multiplied in every step:

$$\dots \underbrace{\underbrace{\underbrace{P(7) P(6)}\; \underbrace{P(5) P(4)}}\; \underbrace{\underbrace{P(3) P(2)}\; \underbrace{P(1) P(0)}}}.$$

Why is this better? For simplicity, assume that the entries of P belong to $\mathbb{Z}[x]$, and that $N = 2^k$ for some k. Each of the matrices $P(0), \dots, P(2^k - 1)$ is then an integer matrix whose entries have at most δ digits, with $\delta = \mathrm{O}(\log(N))$. The product of 2^i of these matrices will have entries with at most $2^i \delta$ digits. Therefore, if $T(N)$ is the time to compute the entire product, then $T(N) = 2T(N/2) + \mathrm{O}(r^\omega \mathrm{M}_{\mathbb{Z}}(N\delta))$ where $\mathrm{M}_{\mathbb{Z}}(N\delta)$ is the time needed to multiply two integers with $\leq N\delta$ digits. The recurrence implies $T(N) = \mathrm{O}(r^\omega \mathrm{M}_{\mathbb{Z}}(N\delta) \log(N)) = \mathrm{O}(r^\omega \mathrm{M}_{\mathbb{Z}}(N) \log(N)^2) = \mathrm{O}^\sim(N)$. When fast multiplication is available, it is therefore better to evaluate matrix products in a balanced way, as summarized in the following algorithm.

Algorithm 2.2
Input: *A matrix* $P \in C(x)^{r\times r}$ *and two numbers* $a, b \in \mathbb{N}$ *such that no denominator in* P *vanishes for any* $n \in \{a, a+1, \dots, b-1\}$.
Output: *The matrix product* $P(b-1)\cdots P(a+1)P(a) \in C^{r\times r}$.

if $a = b$*, then*
    Return the identity matrix I_r.
if $a = b + 1$*, then*
    Return $P(a)$.
Set $m = \lfloor (a+b)/2 \rfloor$.
Recursively compute $A = P(m-1)\cdots P(a)$.
Recursively compute $B = P(b-1)\cdots P(m)$.
Return BA.

For an implementation of the algorithm it is advisable to first clear denominators and write $P = p_0^{-1}P_0$ for some $p_0 \in C[x]$ and $P_0 \in C[x]^{r\times r}$, then apply the algorithm to p_0 (viewed as a 1×1-matrix) and P_0 separately, and then combine the outputs.

Example 2.3 Let us compute an approximation of π using the formula

$$\frac{\pi}{2} = \sum_{n=0}^{\infty} \frac{(2n)!!}{(2n+1)!!}\left(\frac{1}{2}\right)^n.$$

The sequence $a_n = \sum_{k=0}^{n} \frac{(2k)!!}{(2k+1)!!}\left(\frac{1}{2}\right)^k$ of partial sums is D-finite; it satisfies the recurrence

$$(2n+5)a_{n+2} - (3n+7)a_{n+1} + (n+2)a_n = 0.$$

Together with the initial values $a_0 = 1$ and $a_1 = 4/3$, the sequence is uniquely determined.

By either Algorithm 2.1 or 2.2 we can find, for example,

$$\begin{aligned}
a_{10} &= \frac{22850816}{14549535},\\
a_{100} &= \frac{3492861\text{(69 digits suppressed)}0285184}{2223624\text{(69 digits suppressed)}9432175},\\
a_{1000} &= \frac{2318117\text{(850 digits suppressed)}7566208}{1475759\text{(850 digits suppressed)}5023125},\\
a_{10000} &= \frac{4677994\text{(8658 digits suppressed)}7056768}{2978104\text{(8658 digits suppressed)}9328125},\\
a_{100000} &= \frac{3662254\text{(86847 digits suppressed)}7058048}{2331463\text{(86847 digits suppressed)}0234375}.
\end{aligned}$$

These terms match the correct value of $\pi/2$ to an accuracy of 10^{-3}, 10^{-32}, 10^{-303}, 10^{-3013}, and 10^{-30106}, respectively. For larger indices, Algorithm 2.1 is no longer pleasant. On the other hand, Algorithm 2.2 has no trouble to also find

$$a_{1000000} = \frac{9303415(868607 \text{ digits suppressed})6563968}{5922738(868607 \text{ digits suppressed})0234375},$$

$$a_{10000000} = \frac{2440358(8686126 \text{ digits suppressed})9748864}{1553580(8686126 \text{ digits suppressed})0078125},$$

$$a_{100000000} = \frac{2742066(86857578 \text{ digits suppressed})2611584}{1745654(86857578 \text{ digits suppressed})3515625},$$

so it is at least one thousand times better in this example. □

As in the example above, a typical motivation for computing the value of a sequence term with a large index is to get some idea about the asymptotic behavior of the sequence, for example, to find a good numerical approximation for the limit of a convergent sequence. Rational numbers may not be the best choice for such computations. For example, the term a_{100000} has an accuracy of about 3000 decimal digits but the numerator and denominator of its exact representation have together more than 170,000 decimal digits, almost sixty times as much. We could use floating point numbers instead of exact rational numbers. This has the advantage that we do not need to worry about expression swell, but it has the disadvantage that we need to worry about error propagation. Suppose we have a D-finite sequence $(a_n)_{n=0}^{\infty}$ which converges to a limit $a \in \mathbb{R}$ for which we want to compute the first N decimal digits. Also assume that the recurrence satisfied by the sequence only involves coefficients that are much shorter than N digits. We can then apply Algorithm 2.1 with the exact recurrence and a vector of approximate initial values. In each iteration, we may lose some of the accuracy, so we should not iterate too much. On the other hand, we want to approximate the limit, so we should not iterate too little either.

Example 2.4 Consider again the sequence $(a_n)_{n=0}^{\infty}$ from Example 2.3. For the purpose of a more dramatic effect, let us use the alternative recurrence

$$\begin{aligned}&(2n+7)(3n+8)a_{n+3} - (21n^2+128n+190)a_{n+2}\\&+ (21n^2+125n+178)a_{n+1} - 2(n+2)(3n+11)a_n = 0.\end{aligned}$$

Applying Algorithm 2.1 to this recurrence and initial values approximated to an accuracy of 50 decimal places, we obtain the following approximate values for the subsequent terms:

$$
\begin{aligned}
a_{10} &\approx \underline{1.570}55301080006888192646706578595123486764353637\utilde{929},\\
a_{20} &\approx \underline{1.570796}14937016981635096124801212944004723\utilde{5310766},\\
a_{30} &\approx \underline{1.570796326}6505798615040073497528911380788\utilde{5505542985},\\
a_{40} &\approx \underline{1.570796326794}773296743164692121130264\utilde{3852303007029},\\
a_{50} &\approx \underline{1.570796326794896}51082777352681361\utilde{5037854543027 4151},\\
a_{60} &\approx \underline{1.570796326794896619}134267054029\utilde{40464539774844 76396},\\
a_{70} &\approx \underline{1.5707963267948966192311}233670\utilde{5496786544198531121923},\\
a_{80} &\approx \underline{1.570796326794896619231321 6}\utilde{7149133712318148679729 98},\\
a_{90} &\approx \underline{1.570796326794896619231 3}\utilde{835885673753818209445675098},\\
a_{100} &\approx \underline{1.57079632679489661929}\utilde{4704221651093938405064373781 9},\\
a_{110} &\approx \underline{1.5707963267948966}\utilde{841350324233250967344296829680409},\\
a_{120} &\approx \underline{1.570796326794}\utilde{9630806311109374333966323914182635029}.
\end{aligned}
$$

Underlined digits agree with the digits of the limit $\pi/2$. Digits marked with a squiggly line differ from the correct digits of the respective terms because of accumulated numerical errors. The best approximation among the listed terms is a_{80}. Earlier terms are less close to the limit while later terms are blurred by too much noise. □

In practice, the effect is usually not as strong as for the (artificially constructed) recurrence used in the example. If we had used the recurrence stated in Example 2.3, we would have hardly observed any error propagation (see Exercise 3 in Sect. 2.4). A vector of approximate initial values $(\tilde{a}_0, \ldots, \tilde{a}_{r-1})$ can be viewed as the sum of the exact initial values $(a_0, \ldots, a_{r-1})$ and a noise vector $(\epsilon_0, \ldots, \epsilon_{r-1})$. If we write $(\tilde{a}_n)_{n=0}^{\infty}$ for the sequence obtained by the recurrence using the initial values $(\tilde{a}_0, \ldots, \tilde{a}_{r-1})$ and $(a_n)_{n=0}^{\infty}$, $(\epsilon_n)_{n=0}^{\infty}$ for the sequences obtained using the exact initial values $(a_0, \ldots, a_{r-1})$ and the noise vector $(\epsilon_0, \ldots, \epsilon_{r-1})$, respectively, then we have $\tilde{a}_n = a_n + \epsilon_n$ for all $n \in \mathbb{N}$. In order to understand how the error can propagate, we need to estimate how much faster $(\epsilon_n)_{n=0}^{\infty}$ can grow than $(a_n)_{n=0}^{\infty}$.

We can estimate the minimal and maximal growth rate of solutions of a recurrence, and hence the worst possible error propagation, in terms of the limiting companion matrix $P := \lim_{n\to\infty} P(n)$. Recall from linear algebra that every matrix $P \in \mathbb{C}^{r\times r}$ can be written in the form $P = U\Sigma V^*$, where $U, V \in \mathbb{C}^{r\times r}$ are unitary matrices and $\Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_r)$ for some $\sigma_1, \ldots, \sigma_r \in \mathbb{R}$ with $\sigma_1 \geq \cdots \geq \sigma_r \geq 0$. Such a factorization is called a *singular value decomposition* of P, and the entries on the diagonal of Σ are called the *singular values* of P. It can be shown that the nonzero squares of the singular values of P are precisely the nonzero eigenvalues of the hermitian positive semi-definite matrix $PP^* \in \mathbb{C}^{r\times r}$. If $\sigma_{\min}$ is the smallest and $\sigma_{\max}$ is the largest singular value of P, then we have

$\sigma_{\min}\|x\| \le \|Px\| \le \sigma_{\max}\|x\|$ for all $x \in \mathbb{C}^n$, where $\|\cdot\|$ denotes the standard Euclidean norm on $\mathbb{C}^r$.

Proposition 2.5 *Assume that $C \subseteq \mathbb{C}$. Let $p_0, \dots, p_r \in C[x]$ be such that $p_r(n) \neq 0$ for all $n \in \mathbb{N}$.*

Let $P(x) \in C(x)^{r\times r}$ be the companion matrix of the recurrence $p_0(n)f(n) + \cdots + p_r(n)f(n+r) = 0$, let $\sigma_-, \sigma_+ \ge 0$ be such that $\sigma_- \le \sigma_{\min}(n)$ and $\sigma_{\max}(n) \le \sigma_+$ for all $n \in \mathbb{N}$, where $\sigma_{\min}(n)$ and $\sigma_{\max}(n)$ denote the smallest and largest singular value of $P(n) \in C^{r\times r}$, respectively.

Let $(a_n)_{n=0}^{\infty}$ be a nonzero solution of the recurrence. Then

$$\sigma_-^n \le \frac{\|(a_n, \dots, a_{n+r-1})\|}{\|(a_0, \dots, a_{r-1})\|} \le \sigma_+^n$$

for every $n \in \mathbb{N}$. □

Proof From $(a_n, \dots, a_{n+r-1}) = P(n-1)\cdots P(0)(a_0, \dots, a_{r-1})$ we get

$$\begin{aligned}\|(a_n, \dots, a_{n+r-1})\| &\le \sigma_{\max}(n-1)\cdots\sigma_{\max}(0)\|(a_0, \dots, a_{r-1})\|\\ &\le \sigma_+^n\|(a_0, \dots, a_{r-1})\|\end{aligned}$$

for every $n \in \mathbb{N}$. This shows the upper bound. The proof of the lower bound is analogous. ■

The lower bound stated in the proposition is only interesting when σ_- is positive. This is the case if and only if every instance $P(n)$ of the companion matrix as well as the limiting matrix $P := \lim_{n\to\infty} P(n)$ are invertible, and this is the case if and only if $p_0(n) \neq 0$ for all $n \in \mathbb{N}$ and $\deg p_0 \ge \deg p_r$. For the upper bound to be meaningful, we need that $\sigma_{\max}(n)$ is bounded as n goes to infinity. This is the case if and only if the limiting matrix P exists, and this is the case if and only if $\deg p_i \le \deg p_r$ for all i. The example $a_n = n!$ shows that a D-finite sequence can grow faster than exponential when there is an $i < r$ with $\deg p_i > \deg p_r$.

The bounds given in Proposition 2.5 are simple but not sharp. The actual growth rates of solutions of a recurrence are more closely related to the eigenvalues of $P(n)$ than to their singular values, but it requires a bit more work to show this (cf. Exercises 3 and 4 in Sect. 2.4). What matters for now is that we have some bound on the growth of D-finite sequences, at least in the case when $\deg p_i \le \deg p_r$ for all i. Since the sequence of errors is also a solution of the recurrence, we have a bound on the amount of accuracy that is lost per iteration: at most $\log_{10}\sigma_+$ decimal digits. This knowledge can be turned into a guarantee that a certain number of digits of a term we computed with approximate arithmetic is correct. An example is given in Exercise 8.

Strictly speaking, the discussion up to this point assumes that we use approximate initial values but then perform the whole computation of the sequence terms with exact arithmetic. Indeed, all we have analyzed is the impact of a slight variation of the initial values on the final result. In an actual computation, we should do the whole computation using approximate numbers, and round not only once at the beginning but after each arithmetic operation. Doing so introduces another source of error. This error is generally small, but it also has to be taken into account if we really want to guarantee a certain number of correct digits. An elegant way of keeping the accumulated rounding error under control is the use of *ball arithmetic*. The idea is to represent a real (or complex) number ξ by a pair $(\bar{\xi}, \epsilon)$, where $\bar{\xi}$ is a real (or complex) number that can be easily represented, for example, by a number of the form $\bar{\xi} = u2^n$ for some $u, n \in \mathbb{Z}$, and ϵ is a small positive number such that ξ belongs to the ball centered at $\bar{\xi}$ with radius ϵ. For every arithmetic operation, we compute not only an approximate number of the result but also a bound on its error given the error bounds of the input. Instead of estimating the accumulated error of a whole computation, a pragmatic approach is to simply choose the accuracy of the initial values slightly higher than what the error analysis above indicates. If it turns out that the ϵ of the final result is larger than the target accuracy, repeat the computation with a higher accuracy of the initial values, and keep increasing the starting accuracy until the final result has the desired accuracy.

Returning to exact arithmetic, there is one more algorithm for fast evaluation of isolated terms. Algorithm 2.1 discussed above is adapted to the situation where intermediate expressions grow. In domains without expression swell, Algorithm 2.2 has no advantage over Algorithm 2.1. (It has also no advantage if classical multiplication is used, but let's assume that fast multiplication is available.) The following algorithm is well suited for domains in which there is no expression swell, for example, if C is a finite field. The idea for this algorithm is a baby-step-giant-step approach: we first compute the matrix $Q(x) := P(x + \lfloor\sqrt{N}\rfloor) \cdots P(x + 2)P(x + 1)$ (baby steps) and then evaluate the entries of this matrix for $x = 0, \lfloor\sqrt{N}\rfloor, 2\lfloor\sqrt{N}\rfloor, \dots, \lfloor\frac{N-r}{\lfloor\sqrt{N}\rfloor}\rfloor\lfloor\sqrt{N}\rfloor$ (giant steps). By

$$P(N-r)\cdots P(1) = \Big(P\big(N-r\big)P\big(N-r-1\big)\cdots P\Big(\big(\lfloor\frac{N-r}{\lfloor\sqrt{N}\rfloor}\rfloor+1\big)\lfloor\sqrt{N}\rfloor+1\Big)\Big)$$
$$\times\Big(Q\big(\lfloor\frac{N-r}{\lfloor\sqrt{N}\rfloor}\rfloor\big)\cdots Q\big(\lfloor\sqrt{N}\rfloor\big)Q\big(0\big)\Big),$$

we can get the desired product of $\approx N$ matrices by performing only $\approx 2\sqrt{N}$ matrix multiplications, once we know the evaluations of Q. For computing these evaluations quickly, we rely on Theorem 1.21, which says that for a given polynomial $u \in C[x]$ with $\deg(u) < d$ and d given points $x_1, \dots, x_d$, the computation of the values $u(x_1), \dots, u(x_d)$ costs no more than $\mathrm{O}(\mathrm{M}(d)\log(d))$ operations in the ground field. To compute the polynomial matrix Q in the first place, we can use the following variation of repeated squaring.

Algorithm 2.6
Input: *A matrix* $P \in C[x]^{r\times r}$ *and an integer* $s \in \mathbb{N}$.
Output: *The matrix product* $P(x+s)P(x+s-1)\cdots P(x) \in C[x]^{r\times r}$.

1 *if* $s = 0$, *then*
2   *Return the identity matrix* I_r.
3 *else if* $s = 1$, *then*
4   *Return* P.
5 *Set* $t = \lfloor s/2 \rfloor$ *and compute* $\tilde{P} := P(x+t-1)P(x+t)\cdots P(x)$ *recursively.*
6 *Set* $\tilde{P} := \tilde{P}(x+t)\,\tilde{P}(x)$.
7 *if* $2t \neq s$, *then*
8   *Set* $\tilde{P} := P(x+s)\,\tilde{P}$.
9 *Return* $\tilde{P}$.

Lemma 2.7 *Algorithm 2.6 is correct and requires no more than* $\mathrm{O}(r^{\omega}\mathrm{M}(sd)\log(s))$ *operations in* C *when applied to a matrix whose entries are polynomials of degree at most* d.

Proof The correctness is easy to confirm. For the complexity, the two costly operations in each recursion level are the shifts $\tilde{P}(x) \to \tilde{P}(x+t)$ in line 6 and the matrix multiplication $\tilde{P}(x+t)\,P(x)$, also in line 6. At the top level of the recursion, the matrices $\tilde{P}(x)$ and $\tilde{P}(x+t)$ have entries of degrees at most $td = \mathrm{O}(sd)$. According to Theorem 1.21, the shift costs $\mathrm{O}(r^2\mathrm{M}(sd))$. The matrix multiplication costs $\mathrm{O}(r^{\omega}\mathrm{M}(sd))$. For the total cost $T(s)$ of the algorithm we therefore have the recursion $T(s) = T(s/2) + \mathrm{O}(r^{\omega}\mathrm{M}(sd))$, which has the solution stated in the theorem. ■

We are ready to state the improved evaluation algorithm.

Algorithm 2.8
Input: *A D-finite sequence* $(a_n)_{n=0}^{\infty}$ *specified by a recurrence equation* $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ *with* $p_r(n) \neq 0$ *for* $n \in \mathbb{N}$ *and initial values* $a_0, a_1, \ldots, a_{r-1}$; *an integer* $N \in \mathbb{N}$.
Output: *The term* a_N.

if $N < 2r$, *then*
    Use Algorithm 2.1.
Set $s = \lfloor\sqrt{N}\rfloor$ *and* $t = \lfloor\frac{N-r}{s}\rfloor$.
Let $$P := \begin{pmatrix} 0 & p_r & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & p_r \\ -p_0 & -p_1 & \cdots & \cdots & -p_{r-1} \end{pmatrix} \in C[x]^{r\times r} \text{ and } p = p_r \in C[x]^{1\times 1}.$$
Compute $Q(x) = P(x+s-1)\cdots P(x) \in C[x]$ *and* $q(x) = p(x+s-1)\cdots p(x) \in C[x]^{1\times 1}$ *using Algorithm 2.6.*
Compute $Q(0), Q(s), \ldots, Q((t-1)s) \in C^{r\times r}$ *and* $q(0), q(s), \ldots, q((t-1)s) \in C$ *using fast multipoint evaluation.*

7 *Compute* $P(ts), \ldots, P(N-r) \in C^{r \times r}$ *and* $p(ts), \ldots, p(N-r)$ *using fast multipoint evaluation.*

8 *Compute the vector*

$$\begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} := \big(P(N-r) \cdots P(ts+1)\big)\big(Q(t) \cdots Q(0)\big) \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix} \in C^r.$$

9 *Return* $v_r \big/ \big(p(N-r) \cdots p(ts) q(s(t-1)) \cdots q(0)\big) \in C$.

Theorem 2.9 *Algorithm 2.8 is correct and requires no more than* $\mathrm{O}(r^\omega \mathrm{M}(d\sqrt{N}) \log(N)^2)$ *field operations.* □

Proof The correctness follows from the discussion before Algorithm 2.6. For the complexity, we have to argue that the computation time is dominated by line 5, which, according to Lemma 2.7, has the announced cost. Nothing costly happens in lines 1–4. The fast multipoint evaluation in line 6 has to be applied $r^2 + 1$ times (for r^2 matrix entries and one scalar instance for the denominator). Each of these computations can be done with $\mathrm{O}(\mathrm{M}(d\sqrt{N}) + \mathrm{M}(\sqrt{N}) \log(N))$ operations in C. First, replace each polynomial with its remainder mod $x(x+1) \cdots (x+t)$: this costs $\mathrm{O}(\mathrm{M}(d\sqrt{N}))$ operations and reduces all of the degrees to $\mathrm{O}(\sqrt{N})$. Then, apply simultaneous evaluation (part 4 of Theorem 1.21): this costs $\mathrm{O}(\mathrm{M}(\sqrt{N}) \log(N))$ operations. Altogether, line 6 requires no more than $\mathrm{O}(r^2 \mathrm{M}(d\sqrt{N}) \log(N))$ operations in C. The same argument (and thus also the same estimate) applies to line 7. Line 8 requires only $\mathrm{O}(r^\omega \sqrt{N})$ operations. The cost of line 9 is even less: $\mathrm{O}(\sqrt{N})$. ■

Example 2.10 Let us once more consider the recurrence

$$(2n+5)a_{n+2} - (3n+7)a_{n+1} + (n+2)a_n = 0$$

from Example 2.3, together with the initial values $a_0 = 1$ and $a_1 = 4/3$. We want to compute sequence terms of high indices, but to avoid expression swell, let us do the computations in the finite field $\mathbb{Z}_{9223372036854775783}$. Then all intermediate results have a fixed length, and we can use Algorithm 2.9 to compute isolated sequence terms rather quickly. Indeed, an implementation of this algorithm easily finds

$$\begin{aligned} a_{10000000000} &= 8377183736682513170 \bmod 9223372036854775783, \\ a_{100000000000} &= 4745501672893874108 \bmod 9223372036854775783, \\ a_{1000000000000} &= 8796189690220386968 \bmod 9223372036854775783, \\ a_{10000000000000} &= 589058455405082708 \bmod 9223372036854775783. \end{aligned}$$

□

Exercises

1. Let $(a_n)_{n=0}^{\infty}$ be defined by $a_0 = a_1 = a_2 = 1$ and

$$(n^2+2n+3)a_n+(4n^2+5n+6)a_{n+1}+(7n^3+8n+9)a_{n+2}+(10n^2+11n+12)a_{n+3} = 0.$$

Compute a_{100000} by (your own implementations of) all algorithms discussed in this section.

2. Extend Algorithm 2.1 to inhomogeneous recurrences. Suppose that the right hand side is any sequence $(b_n)_{n=0}^{\infty}$ for which an algorithm is known to compute the nth term b_n for any given $n \in \mathbb{N}$.

3****.** Explain how Algorithm 2.2 could be used to compute terms of a solution of an inhomogeneous recurrence. Suppose that the right hand side is itself a D-finite sequence.

4****.** Suppose $(a_n)_{n=0}^{\infty}$ is a D-finite integer sequence with $0 \leq a_n \leq 2^n$ for all $n \in \mathbb{N}$. For some large $N \in \mathbb{N}$, we want to compute a_N using Algorithm 2.1. In order to speed up the computation, we first compute a_N modulo several small primes and then reconstruct the value of a_N by the Chinese remainder theorem. Is this a good idea?

5. Let $(a_n)_{n=0}^{\infty}$ be the sequence from Example 2.3, and let $b_n = a_{2n}$ for $n \in \mathbb{N}$. Since $(a_n)_{n=0}^{\infty}$ satisfies a recurrence of order 2, so does $(b_n)_{n=0}^{\infty}$. In order to evaluate $a_{10000} = b_{5000}$ via Algorithm 2.1, is it better to use the recurrence for $(a_n)_{n=0}^{\infty}$ with $N = 10000$ or the recurrence for $(b_n)_{n=0}^{\infty}$ with $N = 5000$? (You may want to determine the recurrence for $(b_n)_{n=0}^{\infty}$, e.g., by guessing.)

6. For recurrences with constant coefficients, the matrices $P(n)$ have constant entries. Then $P(n)P(n-1)\cdots P(1) = P(1)^n$ can be computed efficiently using repeated squaring. Use this to compute the 20 least significant digits of $F_{2^{1000}}$, where F_n is the n-th Fibonacci number.

7***.** Show that the singular values of the companion matrix $P(n)$ of a recurrence $p_0(n)f(n) + \cdots + p_r(n)f(n+r) = 0$ with $r \geq 2$ and $p_r(n) \neq 0$ for all $n \in \mathbb{N}$ are 1 and

$$\frac{1}{|p_r(n)|}\sqrt{\frac{1}{2}\left(\sum_{i=0}^{r}|p_i(n)|^2 \pm \sqrt{\left(\sum_{i=0}^{r}|p_i(n)|^2\right)^2 - 4|p_0(n)|^2}\right)}.$$

8***.** We want to use the recurrence of Example 2.4 to calculate $\pi/2$ using approximate arithmetic. How many terms do we need and which accuracy should we choose for the initial values in order to guarantee that we get the first 100 digits right?

9. Let $p_0, \ldots, p_r \in C[x]$ with $\deg p_i \leq \deg p_r$ for all i and $p_r(n) \neq 0$ for all $n \in \mathbb{N}$. Let $(a_n)_{n=0}^{\infty}$ be such that $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ for all $n \in \mathbb{N}$. Let $P(x) \in C(x)^{r\times r}$ be the companion matrix of the recurrence and let $\sigma_{\max}(n)$ be the largest singular value of $P(n)$ for $n \in \mathbb{N}$. Let $\sigma_{\max} = \lim_{n\to\infty} \sigma_{\max}(n)$ and let $\epsilon > 0$. Show that there exist $c > 0$ and $n_0 \in \mathbb{N}$ such that $|a_n| < c(\sigma_{\max} + \epsilon)^n \|(a_0, \ldots, a_{r-1})\|$ for all $n \geq n_0$.

10. Let $\xi_1, \xi_2, \bar{\xi}_1, \bar{\xi}_2, \epsilon_1, \epsilon_2$ be such that $|\xi_1 - \bar{\xi}_1| < \epsilon_1$ and $|\xi_2 - \bar{\xi}_2| < \epsilon_2$.
a. Show that $|(\xi_1 + \xi_2) - (\bar{\xi}_1 + \bar{\xi}_2)| < \epsilon_1 + \epsilon_2$
b. Show that $|\xi_1\xi_2 - \bar{\xi}_1\bar{\xi}_2| < |\bar{\xi}_1|\epsilon_2 + |\bar{\xi}_2|\epsilon_1 + \epsilon_1\epsilon_2$

11. Show that 2^{n^2} is not a D-finite sequence.
Hint: Derive a maximal possible order of growth for D-finite sequences from one of the algorithms discussed in this section, and conclude that 2^{n^2} grows too fast.

12. Consider the variant of Algorithm 2.8 obtained by changing line 2 to "$s = \lfloor N^\alpha \rfloor$; $t = \lfloor \frac{N-r}{s} \rfloor$" for some constant α with $0 < \alpha < 1$. Estimate the complexity of the algorithm for arbitrary α. Is there a better choice than $\alpha = \frac{1}{2}$?

13. In Example 2.10, why did the author not choose a smaller modulus, for example 1091, instead of the somewhat bulky prime 9223372036854775783?

References

The idea behind Algorithm 2.2 is known as binary splitting and is a widely used design principle for algorithms in computer algebra exploiting fast multiplication [109, 204]. See Section 12 of Bernstein's survey [59] for some historic remarks. In the context of linear recurrences, the use of balanced matrix products came up in the early 1970s [51, 285]. Improved variants were given by Johansson [251, 252] and Bostan, Gaudry, and Schost [82]. The special case of linear recurrence equations with constant coefficients (cf. Exercise 6) was discussed by Miller and Spencer Brown [329]. They achieve a logarithmic complexity with respect to n, but not with respect to r. An algorithm due to Fiduccia only costs $O(M(r)\log n)$. Bostan and Mori [77] improve Fiduccia's algorithm by a constant factor. Hyun, Melczer, and St-Pierre [244] found an improvement applicable to a restricted class of linear recurrences with constant coefficients.

The bounds on the growth rates based on singular values are simple but crude. Better bounds were given by Mezzarobba and Salvy [327]. An introduction to ball arithmetic was given by van der Hoeven [437]. He also discusses the relation to interval arithmetic, an alternative approach to certified arbitrary-precision numerical computations. Implementations of ball arithmetic are available in Mathemagix [http://www.mathemagix.org] and in Johansson's C-library Arb [250, 253].

The baby-step-giant-step approach is also a widely used general design principle for algorithms in computer algebra. It first arose as a method for finding discrete logarithms and has since found applications to many other problems. The computation of terms of D-finite sequences using baby-step-giant-step algorithms was first proposed by the Chudnovsky brothers [151] and elaborated by Bostan, Gaudry and Schost [82].

2.2 The Solution Space

Properties of the solution space of a recurrence depend heavily on the universe from which the solutions are taken. There are several natural options, and the right one depends on the application. One possibility is to consider the space of all solutions which are sequences $\mathbb{N} \to C$, where C is a field of characteristic zero. A slightly different option is to consider the space of bilateral sequences $\mathbb{Z} \to C$. In the case $C = \mathbb{C}$, a third option is to consider the space of all meromorphic functions which satisfy the recurrence.

In this section we are mainly concerned with sequence solutions. A sequence solution of a recurrence of order r is uniquely determined by a suitable set of initial values. It is clear that the set of all sequence solutions forms a vector space over C. If there are no integer roots in the leading coefficient of the recurrence, we can specify arbitrary values for the terms $a_0, \dots, a_{r-1}$, and the recurrence extends each choice uniquely to an infinite sequence solution. Therefore, the dimension of the solution space is r in this case. More generally, if p_r has integer roots, it can only have finitely many, and one of them must be the largest. If N is the largest integer root, then we can consider the space of all solutions $(a_n)_{n=N}^{\infty}$ in $C^{N+\mathbb{N}}$, and by the same argument, this space will also have dimension r.

We can also consider solutions ranging over all integers. In this case, a particular solution is fixed by a choice of initial values if the recurrence allows us to compute all other terms, both for arbitrarily large as well as for arbitrarily small indices. The easy case is again when there is no trouble with integer roots of the polynomial coefficients of the recurrence.

Proposition 2.11 *Let $p_0, \dots, p_r \in C[x]$ with $p_0, p_r \neq 0$ be such that the smallest integer root of p_0 is N_- and the largest integer root of p_r is N_+. (Take $N_- = \infty$ if p_0 has no integer roots, and $N_+ = -\infty$ if p_r has no integer roots.) Let $V \subseteq C^{\mathbb{Z}}$ be the set of all sequences $(a_n)_{n=-\infty}^{\infty}$ such that*

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$$

for all $n \in \mathbb{Z}$. If $N_+ < N_-$, then V is a C-vector space and $\dim_C V = r$. □

Proof We consider the case $N_- \neq \infty$ and leave the case $N_- = \infty$ to the reader. We show that the linear map $h\colon V \to C^r, h((a_n)_{n=-\infty}^{\infty}) = (a_{N_-}, a_{N_-+1}, \dots, a_{N_-+r-1})$ is an isomorphism of vector spaces.

By the choice of N_-, for every choice $a_{N_-}, a_{N_-+1}, \ldots, a_{N_-+r-1}$ of initial values, the recurrence (applied backwards) gives the values of $a_{N_--1}, a_{N_--2}, \ldots$. Furthermore, because of the assumption $N_+ < N_-$, the recurrence (applied as usual) gives the values of $a_{N_++r}, a_{N_++r+1}, \ldots$. This shows that h is surjective.

h is also injective: suppose that $(a_n)_{n=-\infty}^{\infty}$ is a solution with $a_{N_-} = a_{N_-+1} = \ldots = a_{N_-+r-1} = 0$. By the choice of N_-, we then have $a_n = 0$ for all $n < N_-$. Therefore, if $(a_n)_{n=-\infty}^{\infty}$ is not the zero sequence, there must be a smallest index $N \geq N_-$ such that $a_N \neq 0$. If $N \geq N_- + r$, then $a_{N-r} = \cdots = a_{N-1} = 0$ and $p_r(N-r) \neq 0$ implies $a_N = 0$, which is not possible. But then $N < N_- + r$, and then $(a_0, \ldots, a_{r-1}) \neq 0$, which is not possible either. Therefore $(a_n)_{n=-\infty}^{\infty}$ is the zero sequence. ■

Example 2.12 For the recurrence

$$(n-3)(n+2)a_n + (n^2+5n+2)a_{n+1} + (5n^2-7n+2)a_{n+2} + (n+9)(n+4)a_{n+3} = 0$$

we have $N_- = -2$ and $N_+ = -4$. According to the proposition, the recurrence should have a solution space in $C^{\mathbb{Z}}$ of dimension 3. Indeed, every choice of a_{-2}, a_{-1}, a_0 gives rise to exactly one solution. Choosing (a_{-2}, a_{-1}, a_0) as $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, respectively, we obtain a basis of the solution space:

n	$\cdots$	-4	-3	-2	-1	0	1	2	$\cdots$
$a_n^{(1)}$	$\cdots$	$-\frac{163}{21}$	$\frac{2}{3}$	1	0	0	0	0	$\cdots$
$a_n^{(2)}$	$\cdots$	$-\frac{34}{21}$	$-\frac{34}{3}$	0	1	0	$\frac{2}{7}$	0	$\cdots$
$a_n^{(3)}$	$\cdots$	$-\frac{1}{7}$	-1	0	0	1	$-\frac{18}{7}$	$\frac{19}{12}$	$\cdots$

□

Our next goal is to determine the dimension of the solution space of recurrences for which the condition on N_+ and N_- in Proposition 2.11 is not satisfied. We may assume without loss of generality that $N_- \geq 0$, by replacing a_n with a_{n+c} for a suitable constant $c \in \mathbb{Z}$. This allows us to restrict the attention to indices in $\mathbb{N}$, because every solution valid in this range can be uniquely and indefinitely extended towards negative indices, if desired. Furthermore, we can restrict the attention to indices $n \leq \max(N_+ + r, r-1)$, because for $n > \max(N_+ + r, r-1)$, there is no trouble to compute a_n from earlier values using the recurrence. In summary, it is sufficient to understand what happens for $n = 0, 1, \ldots, \max(N_+ + r, r-1) =: N_{\max}$. These are only finitely many indices. For each of them we want

$$p_0(n)a_n + p_1(n)a_{n+1} + \cdots + p_r(n)a_{n+r} = 0$$

to be satisfied. We can therefore find all suitable choices for $(a_0, \ldots, a_{N_{\max}})$ by solving a linear system. The solution space of the recurrence is isomorphic to the solution space of this linear system. The dimension of the solution space can therefore be determined by the following algorithm.

Algorithm 2.13
Input: $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$.
Output: $\dim_C V$, *where* $V \subseteq C^{\mathbb{N}}$ *is the set of all sequences* $(a_n)_{n=0}^{\infty}$ *such that* $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ *for all* $n \in \mathbb{N}$.

1 *Let* N_+ *be the largest integer root of* p_r, *or* $N_+ = -\infty$ *if* p_r *does not have integer solutions.*
2 *Set* $N_{\max} = \max(N_+ + r, r - 1)$.
3 *Set*

$$M = \begin{pmatrix} p_0(0) & p_1(0) & \cdots\cdots & p_r(0) & & & \\ & p_0(1) & p_1(1) & \cdots\cdots & p_r(1) & & \\ & & \ddots & \ddots & & \ddots & \\ & & & p_0(N_{\max}) & p_1(N_{\max}) & \cdots\cdots & p_r(N_{\max}) \end{pmatrix}.$$

4 *Return* $\dim_C \ker M$.

Theorem 2.14 *Algorithm 2.13 is correct.* □

Proof Consider the linear map $h\colon V \to C^{N_{\max}+r+1}$, $h((a_n)_{n=0}^{\infty}) = (a_0, \ldots, a_{N_{\max}+r})$. This map is injective for the same reason as the map h in the proof of Proposition 2.11. To complete the proof, we show that $\operatorname{im} h = \ker M$.

"$\subseteq$": Let $x \in \operatorname{im} h$, say $h((a_n)_{n=0}^{\infty}) = x$, for some $(a_n)_{n=0}^{\infty} \in V$. Since V is the solution space of the recurrence, the sequence $(a_n)_{n=0}^{\infty}$ satisfies the recurrence for all $n \in \mathbb{N}$, in particular for $n = 0, \ldots, N_{\max}$. Therefore $x \in \ker M$, by the definition of M.

"$\supseteq$": Let $x \in \ker M$, say $x = (a_0, \ldots, a_{N_{\max}+r})$, for certain $a_i \in C$. Then, by the choice of $N_{\max}$, we can use the recurrence to find $a_{N_{\max}+1}, a_{N_{\max}+2}, \ldots$ such that the infinite sequence $(a_n)_{n=0}^{\infty}$ satisfies the recurrence for all $n > N_{\max}$. Furthermore, by the definition of M and because of $x \in \ker M$, this sequence also satisfies the recurrence for $n=0, \ldots, N_{\max}$. We therefore have $(a_n)_{n=0}^{\infty} \in V$ and $h((a_n)_{n=0}^{\infty}) = x$, so $x \in \operatorname{im} h$, as claimed. ■

Example 2.15

1. The solution space of

$$4(n-4)(n-1)a_n - (5n^2 - 37n + 64)a_{n+1} + (n-5)(n-3)a_{n+2} = 0$$

in $\mathbb{Q}^{\mathbb{N}}$ has dimension 4. A basis is given by the following sequences.

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
$a_n^{(1)}$	1	0	$-\frac{16}{15}$	$-\frac{64}{15}$	$-\frac{256}{15}$	0	0	0	0	0	$\cdots$
$a_n^{(2)}$	0	1	$\frac{64}{15}$	$\frac{256}{15}$	$\frac{1024}{15}$	0	0	0	0	0	$\cdots$
$a_n^{(3)}$	0	0	0	0	0	1	4	0	$-\frac{160}{3}$	$-\frac{1000}{3}$	$\cdots$
$a_n^{(4)}$	0	0	0	0	0	0	0	1	$\frac{22}{3}$	$\frac{221}{6}$	$\cdots$

In this case, we may specify arbitrary initial values for the terms a_0 and a_1 at the beginning of the index range as well as for the terms a_5 and a_7 corresponding to the integer roots of the leading coefficient.

2. The solution space of

$$4(n-4)(n+1)a_n - (5n^2 - 37n + 64)a_{n+1} + (n-5)(n-3)a_{n+2} = 0$$

in $\mathbb{Q}^{\mathbb{N}}$ has dimension 2. A basis is given by the following sequences.

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
$a_n^{(1)}$	1	$-\frac{256}{1339}$	$\frac{336}{1339}$	$\frac{576}{1339}$	$\frac{4608}{1339}$	0	0	0	0	0	$\cdots$
$a_n^{(2)}$	0	0	0	0	0	0	0	1	$\frac{22}{3}$	$\frac{203}{6}$	$\cdots$

In this case, we can freely choose a_0 and a_7, but not a_5 or a_6.

3. The solution space of

$$a_n - (2n-9)a_{n+1} + (n-5)(n-3)a_{n+2} = 0$$

in $\mathbb{Q}^{\mathbb{N}}$ has dimension 2. A basis is given by the following sequences.

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
$a_n^{(1)}$	0	0	0	0	0	1	1	0	$-\frac{1}{3}$	$-\frac{5}{24}$	$\cdots$
$a_n^{(2)}$	0	0	0	0	0	0	0	1	1	$\frac{1}{2}$	$\cdots$

In this case, only the values at $n = 5$ and $n = 7$ can be chosen freely, but not those at $n = 0$ or $n = 1$.

□

As can be seen in these examples, it is in general not appropriate to assume that the solution space of a recurrence of order r is generated by r sequences the first r terms of which are $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$, respectively. In the first example, these solutions only generate a proper subspace of the solution space, while in the second and the third examples, no solutions with these initial values exist at all. To see why there cannot be a solution with $a_0 = 1$ and $a_1 = 0$ in these cases, let us have a closer look at what happens when we compute further terms using the recurrence from the second example above. We get $a_2 = \frac{16}{15}$, $a_3 = \frac{64}{15}$, $a_4 = \frac{1024}{45}$. So far no problem. But for determining a_5, the recurrence requires

$$\underbrace{4(3-4)(3+1)\tfrac{64}{15} - (5\cdot 3^2 - 37\cdot 3 + 64)\tfrac{1024}{45}}_{-1024/45} + \underbrace{(3-5)(3-3)}_{0}\,a_5 = 0,$$

and this requirement is violated no matter how we choose a_5. Informally, we can say that setting $a_0 = 1$ and $a_1 = 0$ does not work because with this choice, the computation of a_5 leads to a division by zero. Also in the first example, the attempt to compute a_5 from its predecessors leads to a division by zero. In that case however, the recurrence happens to specialize to $0+0a_5=0$, and this requirement is fulfilled no matter how we choose a_5.

It is perhaps instructive to consider sequence solutions that are defined only for a finite range $\{0,\dots,N\}$. Such a sequence $(a_n)_{n=0}^N$ is a solution of the recurrence if the recurrence is satisfied for all $n=0,\dots,N-r$. Fix a recurrence of order r and write V_N for the space of all its solutions $(a_n)_{n=0}^N$. If $N-r+1$ is not a root of the leading coefficient of the recurrence, then each solution $(a_n)_{n=0}^N \in V_N$ can be uniquely continued to a solution $(a_n)_{n=0}^{N+1} \in V_{N+1}$, so the spaces V_N and V_{N+1} are isomorphic in this case. If $N-r+1$ is a root of the leading coefficient, then only those sequences $(a_n)_{n=0}^N \in V_N$ can be continued for which the recurrence leads to the requirement $0+0a_{N+1}=0$. These sequences form a subspace U of V_N. The sequences in U "survive" the root, while the other solutions "die" at the root. Since the requirement for a solution to survive is just a single linear equation, we always have $\dim_C V_N - 1 \le \dim_C U \le \dim_C V_N$. Moreover, if $N-r+1$ is a root of the leading coefficient, there is also the solution $(a_n)_{n=0}^{N+1}$ with $a_{N+1}=1$ and $a_n=0$ for all $n\le N$. So at every integer root of the leading coefficient, a new sequence is "born", and we have $\dim V_{N+1} = \dim U + 1$, i.e., $\dim V_{N+1} = \dim V_N$ or $\dim V_{N+1} = \dim V_N + 1$. Using these observations, we can prove the following theorem.

Theorem 2.16 *Let $p_0,\dots,p_r \in C[x]$, $p_r \neq 0$, and let $V \subseteq C^{\mathbb{N}}$ be the space of all sequences $(a_n)_{n=0}^\infty$ with*

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$$

for all $n \in \mathbb{N}$. Suppose the nonnegative integer roots of p_r are $s_1,\dots,s_m$. Then $r \le \dim_C V \le r+m$. □

Proof The bound $r \le \dim_C V$ is a consequence of Theorem 2.14: the matrix M in Algorithm 2.13 has $N_{\max}+1$ rows and $N_{\max}+1+r$ columns. Therefore, the dimension of $\ker M$ is at least r.

For the bound $\dim_C V \le r+m$, suppose otherwise that $\dim_C V > r+m$. Then there exist at least $r+m+1$ linearly independent solutions. Then there is a nontrivial linear combination $(a_n)_{n=0}^\infty$ of these solutions which is zero at the $r+m$ indices $0,\dots,r-1, s_1+r,\dots,s_m+r$. As a nontrivial linear combination of linearly independent sequences, $(a_n)_{n=0}^\infty$ is not the zero sequence. Let $N \in \mathbb{N}$ be the smallest index with $a_N \neq 0$. By the choice of $(a_n)_{n=0}^\infty$, we have $N \ge r$ and $N-r \notin \{s_1,\dots,s_m\}$. The recurrence forces $p_0(N-r)0+\cdots+p_{r-1}(N-r)0+p_r(N-r)a_N=0$, which is a contradiction to $p_r(N-r)\neq 0 \neq a_N$. ■

It seems that life would be much easier if there was no danger of dividing by zero. In fact, there is a way to safely avoid divisions by zero. The idea is to introduce an additional parameter q into the recurrence in such a way that all integer roots of the leading coefficient disappear. Formally, instead of a given recurrence with coefficients $p_0,\dots,p_r \in C[x]$, we consider the recurrence whose coefficients are

$\tilde{p}_0, \dots, \tilde{p}_r \in C(q)[x]$, where each $\tilde{p}_i$ is obtained from the corresponding p_i by replacing x with $x+q$. It is clear that $\tilde{p}_r$ cannot have integer roots, because ξ is a root of $\tilde{p}_r$ if and only if $\xi - q$ is a root of p_r, and so if $\tilde{p}_r$ had an integer root, then p_r would have a root involving q, which is impossible since p_r itself does not involve q. The recurrence

$$\tilde{p}_0(n)a_n + \cdots + \tilde{p}_r(n)a_{n+r} = 0$$

therefore has a solution space of dimension r. The solutions are elements of $C(q)^{\mathbb{N}}$, i.e., sequences whose terms are rational functions in q. We can also view them as elements of $C((q))^{\mathbb{N}}$, i.e., sequences whose terms are formal Laurent series in q. If $(a_n)_{n=0}^{\infty}$ is such a solution, then there exists a $k \in \mathbb{N}$ such that $(q^k a_n)_{n=0}^{\infty} \in C[[q]]^{\mathbb{N}}$. The reason is that when $a_n, a_{n+1}, \dots, a_{n+r-1}$ are in $C[[q]]$ but a_{n+r} is not, then we must have $q \mid \tilde{p}_r(n) \in C[q]$, and this can only happen if n is an integer root of p_r. As p_r can only have finitely many integer roots, it follows that there is a finite index $N \in \mathbb{N}$ such that if $a_n \in C[[q]]$ for all $n < N$, then $a_n \in C[[q]]$ for all $n \geq N$. Therefore, it suffices to choose k so that $q^k a_0, \dots, q^k a_N \in C[[q]]$, which is certainly possible.

Conversely, if $(a_n)_{n=0}^{\infty} \in C[[q]]^{\mathbb{N}}$ is a nonzero solution of the deformed recurrence, then there is a unique $k \in \mathbb{N}$ such that $q^{-k}a_n \in C[[q]]$ for all $n \in \mathbb{N}$ but $q^{-k-1}a_n \notin C[[q]]$ for at least one $n \in \mathbb{N}$. Setting $q = 0$ in such a solution, i.e., taking the constant coefficient of each term, we recover a solution in $C^{\mathbb{N}}$ of the original undeformed recurrence. However, not all solutions in $C^{\mathbb{N}}$ can be recovered in this way in general.

Example 2.17

1. Consider the recurrence

$$3(n+2)a_n - (5n-13)a_{n+1} + 2(n-3)a_{n+2} = 0.$$

The deformed recurrence

$$3(n+q+2)a_n - (5(n+q)-13)a_{n+1} + 2(n+q-3)a_{n+2} = 0$$

has a solution space in $\mathbb{Q}(q)^{\mathbb{N}}$ of dimension two and a basis given by the sequences $(a_n^{(1)})_{n=0}^{\infty}$ and $(a_n^{(2)})_{n=0}^{\infty}$ with the following terms:

n	0	1	2	$\cdots$	5	$\cdots$
$a_n^{(1)}$	1	0	$\frac{-3q-6}{2(q-3)}$	$\cdots$	$\frac{-195q^4+\cdots+576}{16(q-3)(q-2)(q-1)q}$	$\cdots$
$a_n^{(2)}$	0	1	$\frac{5q-13}{2(q-3)}$	$\cdots$	$\frac{211q^4+\cdots+2544}{16(q-3)(q-2)(q-1)q}$	$\cdots$

In neither of the two sequences can we set $q = 0$, because some of their terms have denominators which are multiples of q. On the other hand, none of their terms have a denominator which is a multiple of q^2, so we can multiply the sequences by the constant q and then set q to zero. This leads to the following two solutions of the original undeformed recurrence:

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
	0	0	0	0	0	-6	-21	$-\frac{63}{2}$	$-\frac{21}{4}$	$\frac{735}{8}$	$\cdots$
	0	0	0	0	0	$-\frac{53}{2}$	$-\frac{371}{4}$	$-\frac{1113}{8}$	$-\frac{371}{16}$	$\frac{12985}{32}$	$\cdots$

These sequences are linearly dependent. To get another sequence solution, we must observe that the linear combination $\frac{1}{6}a_n^{(1)} - \frac{2}{53}a_n^{(2)}$ has only terms whose denominators are coprime with q. We can therefore set $q = 0$ and obtain

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
	$\frac{1}{6}$	$-\frac{2}{53}$	$\frac{9}{106}$	$\frac{9}{106}$	$\frac{135}{212}$	$\frac{725}{424}$	$\frac{215}{848}$	$-\frac{13935}{1696}$	$-\frac{82405}{3392}$	$-\frac{265105}{6784}$	$\cdots$

This sequence solution together with either of the previous two forms a basis of the solution space in $C^{\mathbb{N}}$ of the unperturbed recurrence.

2. Consider the recurrence

$$3(n-2)a_n - (5n-13)a_{n+1} + 2(n-3)a_{n+2} = 0.$$

The deformed recurrence

$$3(n+q-2)a_n - (5(n+q)-13)a_{n+1} + 2(n+q-3)a_{n+2} = 0$$

has a solution space in $\mathbb{Q}(q)^{\mathbb{N}}$ of dimension two and a basis given by the sequences $(a_n^{(1)})_{n=0}^{\infty}$ and $(a_n^{(2)})_{n=0}^{\infty}$ that start as follows:

n	0	1	2	3	4	5	6	$\cdots$
$a_n^{(1)}$	1	0	$\frac{6-3q}{2(q-3)}$	$\frac{24-15q}{4(q-3)}$	$\frac{72-57q}{8(q-3)}$	$\frac{192-195q}{16(q-3)}$	$\frac{480-633q}{32(q-3)}$	$\cdots$
$a_n^{(2)}$	0	1	$\frac{5q-13}{2(q-3)}$	$\frac{19q-43}{4(q-3)}$	$\frac{65q-129}{8(q-3)}$	$\frac{211q-371}{16(q-3)}$	$\frac{665q-1049}{32(q-3)}$	$\cdots$

In this case, despite the integer root of the leading coefficient of the unperturbed recurrence, no powers of q appear as factors of the denominators in the solutions of the perturbed recurrence. Setting $q = 0$ is legitimate and yields two linearly independent sequence solutions of the unperturbed recurrence. However, the unperturbed recurrence has another sequence solution which cannot be obtained from $a_n^{(1)}$ and $a_n^{(2)}$:

n	0	1	2	3	4	5	6	7	8	$\cdots$
	0	0	0	0	0	1	$\frac{7}{2}$	$\frac{33}{4}$	$\frac{131}{8}$	$\cdots$

□

In view of these examples, the solutions in $C^{\mathbb{N}}$ of a linear recurrence with coefficients in $C[x]$ can be divided into two classes: those solutions which can be obtained by specializing a suitable solution of the deformed recurrence, and those which cannot.

Definition 2.18 Let $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$. Define $\tilde{p}_i(x) = p_i(x+q) \in C(q)[x]$ for $i = 0, \ldots, r$. Then the recurrence

$$\tilde{p}_0(n)a_n + \cdots + \tilde{p}_r(n)a_{n+r} = 0$$

is called the *deformed recurrence* of

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0.$$

A solution $(a_n)_{n=0}^{\infty} \in C^{\mathbb{N}}$ of the latter recurrence is called *robust* if there exists a solution $(\tilde{a}_n(q))_{n=0}^{\infty} \in C[[q]]^{\mathbb{N}}$ of the deformed recurrence such that $a_n = \tilde{a}_n(0)$ for all $n \in \mathbb{N}$. □

Theorem 2.19 *The robust solutions of a recurrence of order r form a C-vector space of dimension r.* □

Proof It is clear that they form a vector space and that the dimension of this space cannot exceed r. We show that its dimension is at least r.

The leading coefficient of the perturbed recurrence has no integer roots, so the solution space in $C((q))^{\mathbb{N}}$ of the perturbed recurrence has dimension r. Therefore, there are $C((q))$-linearly independent solutions $(a_n^{(1)})_{n=0}^{\infty}, \ldots, (a_n^{(r)})_{n=0}^{\infty}$ of the deformed recurrence. We show that these solutions can always be chosen in such a way that setting $q = 0$ gives C-linearly independent sequences. To this end, we show that there exist $C((q))$-linearly independent sequence solutions $(a_n^{(1)})_{n=0}^{\infty}, \ldots, (a_n^{(r)})_{n=0}^{\infty}$ in $C[[q]]^{\mathbb{N}}$ of the deformed recurrence and pairwise distinct indices $n_1, \ldots, n_r \in \mathbb{N}$ with $a_{n_j}^{(i)} = \delta_{i,j}$ for all $i, j = 1, \ldots, r$. Here, $\delta_{i,j}$ denotes the Kronecker symbol.

Let $m \in \{0, \ldots, r\}$ be maximal such that there exist m linearly independent sequence solutions $(a_n^{(1)})_{n=0}^{\infty}, \ldots, (a_n^{(m)})_{n=0}^{\infty}$ in $C[[q]]^{\mathbb{N}}$ of the deformed recurrence and pairwise distinct indices $n_1, \ldots, n_m \in \mathbb{N}$ with $a_{n_j}^{(i)} = \delta_{i,j}$ for all $i, j = 1, \ldots, m$. We show that $m = r$. Suppose otherwise that $m < r$. Since the solution space of the deformed recurrence in $C((q))^{\mathbb{N}}$ has dimension r, there is some solution $(a_n)_{n=0}^{\infty}$ in $C[[q]]^{\mathbb{N}}$ such that $(a_n^{(1)})_{n=0}^{\infty}, \ldots, (a_n^{(m)})_{n=0}^{\infty}$ and $(a_n)_{n=0}^{\infty}$ are linearly independent over $C((q))$. Then the solution $(b_n)_{n=0}^{\infty}$ in $C[[q]]^{\mathbb{N}}$ defined by

$$b_n = a_n - (a_{n_1} a_n^{(1)} + \cdots + a_{n_m} a_n^{(m)}) \qquad (n \in \mathbb{N})$$

is not the zero sequence. Then, multiplying by q^k for a suitable $k \in \mathbb{Z}$ gives a sequence in $C[[q]]$ which yields a nonzero sequence in C when setting $q = 0$. Let $n_{m+1} \in \mathbb{N}$ be some index where this sequence in C is nonzero. Then $q^k b_{n_{m+1}} \in C[[q]]$ admits a multiplicative inverse and we can define the solution $(c_n)_{n=0}^{\infty} \in C[[q]]^{\mathbb{N}}$ by setting $c_n = \frac{q^k b_n}{q^k b_{n_{m+1}}} = \frac{b_n}{b_{n_{m+1}}} \in C[[q]]$ for all $n \in \mathbb{N}$. Then, by construction, $c_{n_1} = \cdots = c_{n_m} = 0$ and $c_{n_{m+1}} = 1$. We can now construct a contradiction to the assumed maximality of m: the solutions $(a_n^{(i)} - a_{n_{m+1}}^{(i)} c_n)_{n=0}^{\infty}$ for $i = 1, \ldots, m$ and $(c_n)_{n=0}^{\infty}$ provide a counterexample. ■

For computing a basis of the space of robust solutions, we can use the following algorithm, which has some similarities with the algorithms discussed in Sect. 1.6. It computes a basis of the solution space in $C((q))^{\mathbb{N}}$ of the deformed recurrence by unrolling the recurrence, and for each new term, it eliminates any negative powers of q that may have occurred. The algorithm works with truncated formal Laurent series. The truncation order is chosen so as to ensure that at least the coefficients of terms with negative exponents are correct. As we know that divisions by q originate from integer roots of the leading coefficient, the sum of the multiplicities of the integer roots of the leading coefficient is a suitable choice for the truncation order.

Algorithm 2.20
Input: $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$, *and a number* $N \in \mathbb{N}$ *which is larger than the largest integer root of* p_r
Output: *A basis of the space of all robust solutions of* $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ *where each basis element is represented by its first* $N + r$ *terms.*

Let $s \in \mathbb{N}$ *be the sum of the multiplicities of the integer roots of* p_r.
Set $b_{i,n} = \delta_{i,n} + \mathrm{O}(q^{s+1})$ *for* $i, n = 0, \ldots, r-1$.
for $n = 0, \ldots, N$ *do*
  Set $b_{i,n+r} = -\frac{1}{p_r(n+q)}(p_0(n+q)b_{i,n} + \cdots + p_{r-1}(n+q)b_{i,n+r-1})$ *for* $i = 0, \ldots, r-1$.
  Choose $i \in \{0, \ldots, r-1\}$ *for which the smallest exponent* ν *of* q *in* $b_{i,n+r}$ *is minimal.*
  while $\nu < 0$ *do*
    for $j = 0, \ldots, r-1$ *with* $i \neq j$ *do*
      Set $b_{j,k} = b_{j,k} - \frac{[q^\nu]b_{j,n+r}}{[q^\nu]b_{i,n+r}} b_{i,k}$ *for* $k = 0, \ldots, n+r$.
    Set $b_{i,k} = q b_{i,k}$ *for* $k = 0, \ldots, n+r$, *and set* $\nu = \nu + 1$.
Return $(b_{i,0}(0), \ldots, b_{i,N+r}(0))$ *for* $i = 0, \ldots, r-1$.

Theorem 2.21 *Algorithm 2.20 is correct.* □

Proof It is clear that the algorithm terminates and that it only returns robust solutions. In view of Theorem 2.19, it is therefore enough to show that the solutions returned by the algorithm are linearly independent. We show by induction that when the vectors $(b_{i,0}(0), \dots, b_{i,n+r-1}(0))$ for $i = 0, \dots, r-1$ are linearly independent at the beginning of an iteration of the main loop (i.e., right before line 4), then the vectors $(b_{i,0}(0), \dots, b_{i,n+r}(0))$ for $i = 0, \dots, r-1$ are linearly independent at the end of this iteration (i.e., right after the while loop).

The basis of the induction is secured by line 2. For the induction step, first note that the induction hypothesis implies that right after step 4, the vectors $(b_{j,0}(0), \dots, b_{j,n+r-1}(0), [q^\nu]b_{j,r})$ for $j = 0, \dots, r-1$ are linearly independent. We can now show that the while loop maintains this linear independence, while ν keeps growing. Indeed, after the first round of applying the updates in line 8, the vectors $(b_{j,0}(0), \dots, b_{j,n+r-1}(0), [q^\nu]b_{j,r})$ for $j = 0, \dots, r-1$ will still be linearly independent (in fact even when the last coordinate is dropped), and also after performing step 9, where we have $(b_{i,0}(0), \dots, b_{i,n+r-1}(0), [q^\nu]b_{i,n+r}) = (0, \dots, 0, [q^\nu]b_{i,n+r})$ with the last coordinate being nonzero. The end of the first iteration thus leaves us with $r-1$ vectors whose first $n+r$ coordinates are linearly independent and one vector whose first $n+r$ coordinates are zero and whose $(n+r+1)$st coordinate is nonzero. In any subsequent iteration of the while loop (if there are any), line 8 will not affect $b_{j,k}$ for any $i \neq j$ and any $k < n+r$, so the linear independence is maintained throughout the loop. ■

Besides asking for sequence solutions with support in $\mathbb{N}$ or $\mathbb{Z}$, it is sometimes also of interest to ask for meromorphic solutions of a recurrence. For given polynomials $p_0, \dots, p_r \in C[x]$, the task is then to determine the set of all meromorphic functions $a\colon \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ such that

$$p_0(z)a(z) + p_1(z)a_1(z+1) + \cdots + p_r(z)a_r(z+r) = 0$$

for all $z \in \mathbb{C} \cup \{\infty\}$. Clearly, the set of solutions is a vector space over $\mathbb{C}$, but unlike in the settings discussed before, the dimension of this space is not finite. To see why, consider the simple recurrence $a(z) - a(z+1) = 0$. The set of meromorphic solutions of this recurrence contains the infinite linearly independent set $\{z \mapsto \cos(nz\pi) : n \in \mathbb{N}\}$.

In order to make a useful statement, we need to change the perspective. In the case of sequence solutions, the solutions of the recurrence $a_n - a_{n+1} = 0$ are exactly the constant sequences $c, c, c, \dots$ for some $c \in C$, and we consider solution spaces as vector spaces over C. Analogously, in the context of meromorphic solutions, let $\mathfrak{M}_1$ denote the set of all 1-periodic meromorphic functions, i.e., all of the meromorphic solutions of the recurrence $a(z) - a(z+1) = 0$. Then $\mathfrak{M}_1$ is a subfield of the field $\mathfrak{M}$ of all meromorphic functions, and the solution space of any linear recurrence with polynomial (or, for that matter, meromorphic) coefficients is not only a vector space over $\mathbb{C}$ but even a vector space over $\mathfrak{M}_1$ (Exercise 10). The situation is similar to the solution space in $C((q))^{\mathbb{N}}$ of a deformed recurrence: it is infinite dimensional when we view it as vector space over C, because every solution can be multiplied by any element of $C((q))$.

For every meromorphic solution of a recurrence, there is a finite $k \in \mathbb{Z}$ such that all of its poles in $\mathbb{Z}$ have order at most k. The reason is the same as for the bounded negative powers of q in solutions of deformed recurrences: moving towards the right, the order of poles at two consecutive integers can only increase at roots of the leading coefficients, of which there are at most finitely many; likewise, moving towards the left, the order of poles at two consecutive integers can only increase at roots of the trailing coefficient, of which there are also at most finitely many. By multiplying a given meromorphic solution by a suitable integer power of the function $z \mapsto \sin(\pi z)$ (which belongs to $\mathfrak{M}_1$ and has simple roots at all $z \in \mathbb{Z}$), we can remove all poles in $\mathbb{N}$ and ensure that the restriction of z to $\mathbb{N}$ does not yield the zero sequence.

Each sequence solution obtained in this way is a robust solution in the sense of Definition 2.18. To see this, it suffices to observe that every meromorphic solution $a(z)$ gives rise to a sequence solution $(a_n)_{n=0}^{\infty}$ in $\mathbb{C}((x))^{\mathbb{N}}$ by letting each term a_n be the Laurent series expansion of $a(z)$ at the point $z = n$. Also the converse is true: every robust solution can be obtained by restricting the domain of a meromorphic solution to $\mathbb{N}$. This direction is a consequence of the following theorem, the proof of which is beyond the scope of this book.

Theorem 2.22 *Let $p_0, \dots, p_r \in \mathbb{C}[x]$, $p_r \neq 0$, and let V the set of all meromorphic functions $a\colon \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ such that*

$$p_0(z)a(z) + p_1(z)a(z+1) + \cdots + p_r(z)a(z+r) = 0$$

for all $z \in \mathbb{C}$. Then $\dim_{\mathfrak{M}_1} V = r$, where $\mathfrak{M}_1$ denotes the field of all 1-periodic meromorphic functions. □

Example 2.23 The recurrence $a(z+1) - za(z) = 0$ has the Gamma function $\Gamma(z)$ among its solutions. This function has simple poles at the non-positive integers, so it does not give rise to a sequence solution defined in $\mathbb{Z}$. Since $\sin(2\pi z)$ is a "constant", $\sin(2\pi z)\Gamma(z)$ is also a solution of the recurrence. This function is defined for all integers, and it gives rise to the sequence solution

$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
$\cdots$	$-\frac{\pi}{60}$	$\frac{\pi}{12}$	$-\frac{\pi}{3}$	π	-2π	2π	0	0	0	0	$\cdots$

□

Meromorphic functions form a field. We can consider more generally the situation where we are looking for solutions of a recurrence in some field K. In order to make this meaningful, we need to know how the shift acts on elements of K. The role of the shift will be played by an automorphism which we associate to K.

Definition 2.24 Let R be a commutative ring and let $\sigma\colon R \to R$ be an automorphism.

1. The pair (R, σ) is called a *difference ring*. If R is a field, it is called a *difference field*.

2. An element $c \in R$ is called a *constant* if $\sigma(c) = c$. The set of all constants of R is denoted by $\mathrm{Const}(R)$.
3. If (E, ϕ) is a difference ring such that R is a subring of E and $\phi|_R = \sigma$, then (E, ϕ) is called a *difference ring extension* of (R, σ). If R and E both are fields, we call (E, ϕ) a *difference field extension* of (R, σ). □

We will take the freedom to simply write R instead of (R, σ) when σ is clear from the context. Also, for a difference ring extension (E, ϕ) of a difference ring (R, σ), we will often use the same name for ϕ and σ. It is easy to show that $\mathrm{Const}(R)$ is always a subring of R, it is called the constant ring of R. If R is a field, then $\mathrm{Const}(R)$ is also a field and it is called the constant field of R.

Examples for difference fields include the rational function field $C(x)$ with $\sigma\colon C(x) \to C(x)$ defined by $\sigma(r(x)) = r(x + 1)$. Then the constant field of $C(x)$ is C. Unless otherwise stated, we will always assume that $C(x)$ is equipped with this automorphism σ. Another common way to turn $C(x)$ into a difference field is by defining $\sigma\colon C(x) \to C(x)$ through $\sigma(r(x)) = r(qx)$ for some fixed $q \in C$. If C is a subfield of $\mathbb{C}$, then the field of meromorphic functions together with the natural shift operation sending x to $x + 1$ is a difference field extension of $C(x)$. Its constant field consists of all the meromorphic functions with period 1. The ring $C^{\mathbb{Z}}$ forms a difference ring if we define σ as the function that takes any sequence $(a_n)_{n\in\mathbb{Z}}$ to $(a_{n+1})_{n\in\mathbb{Z}}$. Also the ring of germs of sequences introduced in Definition 1.9 is a difference ring. A more obscure example for a difference ring is the field $\bigcup_{i\in\mathbb{N}\setminus\{0\}} C((x^{1/i}))$ of Puiseux series together with the automorphism σ defined by $\sigma(x) = x^q$ for some fixed $q > 1$.

If (K, σ) is any difference field extension of $C(x)$, then it is meaningful to ask for solutions in K of a linear recurrence with coefficients $p_0, \ldots, p_r \in C(x)$: these are the elements $y \in K$ for which we have

$$p_0 y + p_1\sigma(y) + \cdots + p_r\sigma^r(y) = 0.$$

Difference fields can be used for characterizing certain types of expressions in "closed form". For example, we can ask for the solutions of a certain recurrence in the difference field $K = C(x, y_1, y_2)$ on which σ is defined by $\sigma(x) = x + 1$, $\sigma(y_1) = (x + 1)y_1$, and $\sigma(y_2) = 2y_2$. In this setting, the variables y_1 and y_2 represent the expressions $x!$ and 2^x, respectively. The closed form expressions returned by algorithms for finding solutions to recurrence equations must always be understood in this way, and care must be applied when these expressions are translated to statements about sequence solutions.

Example 2.25

1. Let the sequence $(a_n)_{n=0}^{\infty}$ be defined by $a_0 = 2$, $a_1 = 7$, $a_2 = 27$, and

$$\begin{aligned}&(n + 3)^2 a_{n+3} - 2(6n^2 + 28n + 33)a_{n+2}\\ &+ 4(2n + 3)(6n + 11)a_{n+1} - 16(2n + 1)(2n + 3)a_n = 0.\end{aligned}$$

In a suitably defined difference field, the recurrence admits the closed form solutions 4^x and $\binom{2x}{x}$. It is easy to check that the corresponding sequences $(4^n)_{n=0}^{\infty}$ and $(\binom{2n}{n})_{n=0}^{\infty}$ are also solutions. In order to check whether $(a_n)_{n=0}^{\infty}$ is a linear combination of those, we can set up and solve a linear system. If $a_n = c_1 4^n + c_2\binom{2n}{n}$ is true for all $n \in \mathbb{N}$, it must be true for $n = 0$ and $n = 1$. This gives an inhomogeneous linear system for c_1 and c_2 with the unique solution $(c_1, c_2) = (3/2, 1/2)$. Therefore we have $a_n = \frac{3}{2}4^n + \frac{1}{2}\binom{2n}{n}$ for all $n \in \mathbb{N}$.

2. Consider the recurrence

$$3(n-2)a_n - (5n-13)a_{n+1} + 2(n-3)a_{n+2} = 0,$$

which already appeared in Example 2.17. There are two closed form solutions $x-1$ and $(3/2)^x$, but the solution space in $C^{\mathbb{N}}$ has dimension three. So there is at least one sequence solution which is not a linear combination of $(n-1)_{n=0}^{\infty}$ and $((3/2)^n)_{n=0}^{\infty}$.

□

We show next that the size of the solution space of a recurrence in a difference field is limited.

Theorem 2.26 *(See Theorem 3.20 for the differential case) Let (K, σ) be a difference field, and let $p_0, \ldots, p_r \in K$ with $p_r \neq 0$. Let*

$$V = \{\, y \in K : p_0 y + p_1\sigma(y) + \cdots + p_r\sigma^r(y) = 0 \,\} \subseteq K.$$

Then V is a vector space over Const(K) *of dimension at most r.* □

Proof It is easy to check that V is a vector space over Const(K). To show the bound on the dimension, let $y_0, \ldots, y_r \in V$. We show that they are linearly dependent over Const(K). In fact, we will show that the vectors $Y_i = (y_i, \sigma(y_i), \ldots, \sigma^{r-1}(y_i)) \in K^r$ are linearly dependent over Const(K). It is clear that they are linearly dependent over K, because $r+1$ elements of K^r are always linearly dependent over K.

Let k be minimal such that $Y_0, \ldots, Y_k$ are linearly dependent over K, and let $c_0, \ldots, c_{k-1} \in K$ be such that we can write $Y_k = \sum_{i=0}^{k-1} c_i Y_i$.

Set

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \ldots & 0 & 1 \\ -p_0/p_r & -p_1/p_r & \cdots & \cdots & -p_{r-1}/p_r \end{pmatrix},$$

so that $\sigma(Y_i) = AY_i$ for $i = 0, \ldots, r$.

Now we have

$$\sigma(Y_k) = \sum_{i=0}^{k-1} \sigma(c_i)\sigma(Y_i)$$

on the one hand, and

$$\sigma(Y_k) = AY_k = A\sum_{i=0}^{k-1} c_i Y_i = \sum_{i=0}^{k-1} c_i AY_i = \sum_{i=0}^{k-1} c_i \sigma(Y_i)$$

on the other hand. Subtracting these two equations gives $\sum_{i=0}^{k-1}(\sigma(c_i) - c_i)\sigma(Y_i) = 0$. By the minimality of k, it follows that $\sigma(c_i) = c_i$ for $i = 0, \ldots, k-1$, and therefore, $c_i \in \mathrm{Const}(K)$ for all i, as claimed. ∎

Let K be a difference field with constant field $\mathrm{Const}(K) = C$, and consider a linear recurrence equation $p_0 y + \cdots + p_r \sigma^r(y) = 0$ with coefficients in K. Assume that r is chosen such that $p_r \neq 0$. It is possible to construct a difference field extension E of K such that the solutions in E of the equation form a vector space over C of arbitrarily large dimension. For instance, to obtain the dimension $d \in \mathbb{N}$, let E be the rational function field over K with the variables $y_{i,j}$ ($i = 1, \ldots, d$, $j = 0, \ldots, r-1$) and extend the automorphism σ from K to E via $\sigma(y_{i,j}) = y_{i,j+1}$ for $i = 1, \ldots, d$ and $j = 0, \ldots, r-2$ and $\sigma(y_{i,r-1}) = -\frac{1}{p_r}(p_0 y_{i,0} + \cdots + p_{r-1} y_{i,r-1})$ for $i = 1, \ldots, d$. Then $\{y_{1,0}, \ldots, y_{d,0}\}$ is a set of d solutions in E which is linearly independent over C.

The apparent contradiction to Theorem 2.26 is resolved by observing that the constant field of the extended field E may be larger than C. For example, consider the equation $\sigma(y) + y = 0$ with $K = C = \mathbb{Q}$. Following the construction sketched above, we would take $E = K(y)$ with $\sigma(y) = -y$. Then $\sigma(y^2) = \sigma(y)^2 = (-y)^2 = y^2$, so $y^2 \in \mathrm{Const}(E)$ while $y^2 \notin C$. We call a constant in $E \setminus \mathrm{Const}(K)$ a *fake constant,* because in applications we are only interested in difference field extensions E with $\mathrm{Const}(E) = \mathrm{Const}(K)$, i.e., the extended difference field should only contain "true constants".

According to Theorem 2.26, in a difference field extension with no fake constants the solution space of a given recurrence cannot exceed the order of the recurrence. However, it can be smaller. As an example, consider the equation $\sigma^2(y) - 3\sigma(y) + 2y = 0$ with $K = C = \mathbb{Q}$. If we take $E = C(x)$ with $\sigma(x) = x + 1$, then $\mathrm{Const}(E) = C$ and the solution space of the equation in E is generated by $\{1\}$, i.e., its dimension is only one. In this case, the extension was not well chosen. If we take $E = C(x)$ with $\sigma(x) = 2x$ instead, then $\mathrm{Const}(E) = C$ and the solution space is generated by $\{1, x\}$, so the dimension meets the bound.

Unfortunately, there are recurrence equations for which there does not exist any difference field extension E without fake constants, in which the solution space of the recurrence over C has the order of the recurrence as its dimension. An example is the recurrence $\sigma(y) + y = 0$ with $K = C = \mathbb{C}$. If there was a difference field extension E with no fake constants but containing some nonzero element $y \in E$ such that $\sigma(y) + y = 0$, then $\sigma(y^2) = y^2$ and $\mathrm{Const}(E) = C$ would imply that there exists $c \in \mathbb{C}$ with $y^2 - c = 0$. Since $\mathbb{C}$ is algebraically closed, this in turn would imply that there exist $c_1, c_2 \in \mathbb{C}$ with $(y - c_1)(y - c_2) = 0$. Since y is nonzero and $\sigma(y) = -y$, we know that y itself is not a constant, hence $y - c_1 \neq 0$ and $y - c_2 \neq 0$. But this is impossible because E was assumed to be a field.

In order to cover such cases, we would like to have a version of Theorem 2.26 that works for difference rings instead of fields. There is no hope that a theorem like this could work for any ring, as we have already seen that in the ring $C^{\mathbb{N}}$, the dimension of the solution space of a recurrence can exceed the order. But the following version is sometimes useful.

Theorem 2.27 *Let (K, σ) be a difference field. Let (R, σ) be a difference ring extension of (K, σ) which can be written as $R = g_1K + g_2K + \cdots + g_mK$ for some generators $g_1, \ldots, g_m \in R$ with*

1. $g_1 + \cdots + g_m = 1$,
2. $g_k^2 = g_k$ *for all* k,
3. $g_i g_j = 0$ *for all* $i \neq j$,
4. $\sigma(g_k) = g_{k+1}$ *for* $k = 1, \ldots, m-1$, *and* $\sigma(g_m) = g_1$.

Suppose that $\mathrm{Const}(R) = \mathrm{Const}(K)$. *Let $p_0, \ldots, p_r \in K$ with $p_0, p_r \neq 0$. Let*

$$V = \{\, y \in R : p_0 y + p_1\sigma(y) + \cdots + p_r\sigma^r(y) = 0 \,\} \subseteq R.$$

Then V is a vector space over $\mathrm{Const}(K)$ *of dimension at most r.* □

Proof Let $y_0, \ldots, y_r \in V$. We show that they are linearly dependent over $\mathrm{Const}(K)$. In fact, we will show that the vectors $Y_i = (\sigma^j(y_i))_{j=0}^{r-1} \in R^r$ are linearly dependent over $\mathrm{Const}(K)$. To see that they are linearly dependent over R, observe that $g_k Y_i \in (g_k K)^r$ for every k and i, and since $g_k K \cong K$, it follows from linear algebra that for every k the vectors $g_k Y_0, \ldots, g_k Y_r \in (g_k K)^r \subseteq R^r$ are linearly dependent over K. It follows that $Y_0, \ldots, Y_r$ are linearly dependent over R.

Let $n \in \{0, \ldots, r\}$ be such that the set $\{Y_0, \ldots, Y_n\}$ is linearly dependent over R but every proper subset is not. Then there are $a_0, \ldots, a_n \in R \setminus \{0\}$ such that $a_n \neq 0$ and $a_n Y_n = \sum_{i=0}^{n-1} a_i Y_i$. Consider the set $I = \{\, a_n \in R \mid \exists\, a_0, \ldots, a_{n-1} : a_n Y_n = \sum_{i=0}^{n-1} a_i Y_i \,\}$. It is clear that I is an ideal of R. Furthermore, I is closed under σ, because $\sum_{i=0}^{n} a_i Y_i = 0$ means $\sum_{i=0}^{n} a_i \sigma^j(y_i) = 0$ for $j = 0, \ldots, r-1$, and applying σ gives $\sum_{i=0}^{n} \sigma(a_i)\sigma^j(y_i) = 0$ for $j = 1, \ldots, r$. Using the recurrence and the assumption $p_0, p_r \neq 0$, this also implies $\sum_{i=0}^{n} \sigma(a_i) y_i = 0$, so $\sum_{i=0}^{n} \sigma(a_i) Y_i = 0$, and thus $\sigma(a_n) \in I$.

Since $I \neq \{0\}$, Exercise 17 yields $1 \in I$, so we have a linear relation of the form $Y_n = \sum_{i=0}^{n-1} \tilde{a}_i Y_i$ for certain $\tilde{a}_i \in R$. From here, we can proceed as in the proof of Theorem 2.26 to show that $\tilde{a}_0, \ldots, \tilde{a}_{n-1} \in \mathrm{Const}(R)$. Because of the assumption $\mathrm{Const}(R) = \mathrm{Const}(K)$, the claim follows. ■

The requirements on the ring R are motivated by *interlaced sequences*. For example, the interlacing of three sequences $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$, $(c_n)_{n=0}^{\infty}$ is defined as the sequence $a_0, b_0, c_0, a_1, b_1, c_1, a_2, b_2, c_2, \ldots$. In the theorem, taking $m = 3$, we would interpret the generators g_1, g_2, g_3 as the sequences $(\delta_{n \bmod 3,0})_{n=0}^{\infty}$, $(\delta_{n \bmod 3,1})_{n=0}^{\infty}$, $(\delta_{n \bmod 3,2})_{n=0}^{\infty}$, respectively. Note that the product of any two of them is the zero sequence, the sum of all of them is the one sequence $(1, 1, 1, 1, \ldots)$, the sequences are invariant under squaring, and shifting one of them gives one of the others.

Example 2.28 Consider the recurrence equation $\sigma(y) + y = 0$ with $K = C = \mathbb{C}$. We want to construct a difference ring R with $\operatorname{Const}(R) = \mathbb{C}$ in which this equation has a solution. Consider $R = g_1K + g_2K$ with $g_1 + g_2 = 1$, $g_1^2 = g_1$, $g_2^2 = g_2$, and $g_1g_2 = 0$. Define $\sigma\colon R \to R$ by $\sigma(\alpha g_1 + \beta g_2) = \beta g_1 + \alpha g_2$. Then (R, σ) is a difference ring extension of (K, id). We have $\sigma(\alpha g_1 + \beta g_2) = \alpha g_1 + \beta g_2$ if and only if $\alpha = \beta$, so $\operatorname{Const}(R) = (g_1 + g_2)K = K$, as desired. Furthermore, $g_1 - g_2$ is a solution of the recurrence, because $\sigma(g_1 - g_2) = -g_1 + g_2 = -(g_1 - g_2)$. Hence the dimension of the solution space in R matches the order of the recurrence. □

Difference rings containing exponential terms can be brought to the form required by Theorem 2.27. Suppose we have a difference field K and some nonzero constants $\phi_1, \ldots, \phi_n$, and we want to construct a difference ring $R = K[\phi_1^x, \ldots, \phi_n^x]$ where the notation ϕ_i^x refers to new elements to which the shift is extended via $\sigma(\phi_i^x) := \phi_i\, \phi_i^x$. If we consider these symbols ϕ_i^x as algebraically independent over K, then this construction in general leads to fake constants. Any such constant can be written as $p(\phi_1^x, \ldots, \phi_n^x)$ for some multivariate polynomial $p \in K[y_1, \ldots, y_n]$. Applying σ to such an expression and equating like terms shows that p must be a finite sum of monomials $uy_1^{e_1} \cdots y_n^{e_n}$ such that $\phi_1^{e_1} \cdots \phi_n^{e_n} = u/\sigma(u)$. If we assume for simplicity that K itself does not have any exponentials, then the right hand side is necessarily 1 (because the left hand side is necessarily constant). We can get rid of all fake constants by discarding the initial assumption that the symbols ϕ_i^x are algebraically independent and imposing instead the algebraic relations $(\phi_1^x)^{e_1} \cdots (\phi_n^x)^{e_n} = 1$ for all $(e_1, \ldots, e_n) \in \mathbb{Z}^n$ with $\phi_1^{e_1} \cdots \phi_n^{e_n} = 1$. For this setting, we have the following variant of Theorem 2.27.

Theorem 2.29 *Let (K, σ) be a difference field with* $\operatorname{Const}(K) = C$. *Suppose that K has no exponential elements, i.e., $\forall\, u \in K \setminus \{0\} : \sigma(u)/u \in \operatorname{Const}(K) \Rightarrow u \in \operatorname{Const}(K)$. Let $\phi_1, \ldots, \phi_n \in C \setminus \{0\}$ and let $R = K[\phi_1^x, \ldots, \phi_n^x]$ be the difference ring extension constructed as described above, i.e., $\sigma(\phi_i^x) = \phi_i\, \phi_i^x$ and $(\phi_1^x)^{e_1} \cdots (\phi_n^x)^{e_n} = 1$ for all $(e_1, \ldots, e_n) \in \mathbb{Z}^n$ with $\phi_1^{e_1} \cdots \phi_n^{e_n} = 1$.*

Let $p_0, \ldots, p_r \in K$ with $p_0, p_r \neq 0$, and

$$V = \{\, y \in R : p_0 y + p_1 \sigma(y) + \cdots + p_r \sigma^r(y) = 0 \,\} \subseteq R.$$

Then V is a vector space over $\operatorname{Const}(K)$ *of dimension at most r.* □

Proof The multiplicative group G generated by $\phi_1, \ldots, \phi_n$ in $C \setminus \{0\}$ is finitely generated and abelian. By the fundamental theorem of finitely generated abelian groups, G is isomorphic to $\mathbb{Z}^k \times H$ for some $k \in \mathbb{N}$ and some finite group H. Moreover, by a general result from field theory (e.g., Lemma 1 in Sect. I§1 of [454] or Thm. 1.9 in Sect. IV§1 of [304]), any finite subgroup of $C \setminus \{0\}$ is cyclic, so we have $H \cong \mathbb{Z}_m$ for some $m \in \mathbb{N}$.

Thanks to these isomorphisms, we may assume without loss of generality that $\phi_1^x, \dots, \phi_{n-1}^x$ are transcendental over K and that ϕ_n is a primitive mth root of unity (otherwise replace the ϕ_i^x by suitable other generators). If $m = 0$, then R is an integral domain and we obtain the desired conclusion by applying Theorem 2.26 to the quotient field of R.

In the case $m > 0$, consider $K' = K(\phi_1^x, \dots, \phi_{n-1}^x)$ and $R' = K'[\phi_n^x]$. For $i = 0, \dots, m-1$, define $g_i = \frac{1}{m}\sum_{j=1}^m (\phi_n)^{ij}(\phi_n^x)^j$. Then $R' = g_0 K' + \dots + g_{m-1}K'$ and $g_0 + \dots + g_{m-1} = 1$ and $g_i^2 = g_i$ for all i and $g_i g_j = 0$ for all $i \neq j$. We also have $\sigma(g_i) = g_{i+1}$ for $i = 0, \dots, m-2$ and $\sigma(g_{m-1}) = g_0$. All these facts are shown in Exercise 18. The claim now follows from Theorem 2.27 applied to R'. ∎

Exercises

1. What is the solution space of the degenerated second order recurrence $a_{n+2} = 0$ **a.** in $\mathbb{Q}^{\mathbb{N}}$, **b.** in $\mathbb{Q}^{\mathbb{Z}}$?

2. Determine a basis of the solution space in $C^{\mathbb{N}}$ of the recurrence

$$(n+1)(2n-3)a_n + 6(n-2)a_{n+1} - (n-3)(2n-5)a_{n+2} = 0.$$

3. Let V and $s_1, \dots, s_m$ be as in Theorem 2.16. Show that V contains a sequence $(a_n)_{n=0}^\infty$ with $a_{s_m+r} = 1$ and $a_n = 0$ for all $n < s_m + r$.

4. Show that the bound $r + m$ in Theorem 2.16 is sharp.

5⋆. Prove or disprove: If $V_{\mathbb{Z}}$ is the solution space in $C^{\mathbb{Z}}$ of a certain recurrence and $V_{\mathbb{N}}$ is the solution space in $C^{\mathbb{N}}$ of the same recurrence, then $\dim_C V_{\mathbb{Z}} \leq \dim_C V_{\mathbb{N}}$.

6⋆. Prove or disprove: If $V_{\mathbb{Z}}$ is the solution space in $C^{\mathbb{Z}}$ of a certain recurrence and $V_{\mathbb{N}}$ is the solution space in $C^{\mathbb{N}}$ of the same recurrence, then $\dim_C V_{\mathbb{Z}} \geq \dim_C V_{\mathbb{N}}$.

7. For the recurrence

$$12a_n + 3(3n-1)a_{n+1} - n(2n+9)a_{n+2} + (n+1)(5n+16)a_{n+3} - 2(n+2)(n+4)a_{n+4} = 0,$$

find a basis of the vector space of all solutions $(a_n)_{n=0}^\infty$ in $\mathbb{Q}^{\mathbb{Z}}$ that have the property $\exists\, N \in \mathbb{Z}\ \forall\, n < N : a_n = 0$.

8. Find all solutions in $\mathbb{C}^{\mathbb{Z}}$ of the recurrence $(n-5)^2(n-3)a_n - (n-4)^2(n-2)a_{n+1} = 0$, and determine a basis of the subspace of robust solutions.

9. Show that a nonzero element of the solution space in $C((q))^{\mathbb{N}}$ of a deformed recurrence of order r cannot contain a run of r consecutive zero terms.

10⋆. Let $\mathfrak{M}_1$ be the field of all meromorphic solutions of the recurrence $a(z) - a(z+1) = 0$. Show that the space of meromorphic solutions of a recurrence

$$p_0(z)a(z) + \cdots + p_r(z)a(z+r) = 0$$

is a vector space over $\mathfrak{M}_1$.

11⋆⋆. Consider a linear recurrence of order r with polynomial coefficients and let V be its solution space in the ring $C^{\mathbb{N}}/\!\sim$ of germs of sequences (cf. Definition 1.9). Show that $\dim_C V = r$.

12⋆. Let F be a finite field and consider a recurrence $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ for some polynomials $p_0, \ldots, p_r \in F[x]$ with $p_r \neq 0$.

a. Show that if $p_r(n) \neq 0$ for all $n \in \mathbb{N}$, then any solution $(a_n)_{n=0}^{\infty}$ of the recurrence is ultimately periodic.

b. Show that if $p_r(n) = 0$ for some $n \in \mathbb{N}$, then the solution space can have infinite dimension and there may be non-periodic solutions.

13. Let K be a difference field, and let $p_0, \ldots, p_r \in K$. Prove or disprove:

a. If there is a $g \in K \setminus \{0\}$ such that the inhomogeneous recurrence $p_0 f + \cdots + p_r\sigma^r(f) = g$ admits a solution f in K, then the homogeneous recurrence $p_0 f + \cdots + p_r\sigma^r(f) = 0$ admits a nonzero solution f in K.

b. If the homogeneous recurrence $p_0 f + \cdots + p_r\sigma^r(f) = 0$ admits a nonzero solution f in K, then for all $g \in K \setminus \{0\}$ the inhomogeneous equation $p_0 f + \cdots + p_r\sigma^r(f) = g$ admits a solution f in K.

c. There always exists a $g \in K$ such that the inhomogeneous equation $p_0 f + \cdots + p_r\sigma^r(f) = g$ admits a solution f in K.

14⋆. Consider the difference field $C(x)$ with $\sigma(x) = x+1$. Show that the constant field of $C(x)$ is C.

15⋆⋆. Consider the difference field $C(x)$ with $\sigma(x) = -x$. Show that the constant field of $C(x)$ is $C(x^2)$.

16. Let p be a prime and consider the difference ring $\mathbb{Z}_p[x]$ with $\sigma(u(x)) = u(x+1)$. Show that $\mathrm{Const}(\mathbb{Z}_p[x]) = \mathbb{Z}_p[x^p - x]$.

17. Let K be a difference field and let R be a difference ring extension which can be written as $R = g_1K + \cdots + g_mK$ for certain $g_1, \ldots, g_m \in R$ with $g_1 + \cdots + g_m = 1$, $g_ig_j = \delta_{i,j}g_i$ for all i, $\sigma(g_i) = g_{i+1}$ for $i < m$, and $\sigma(g_m) = g_1$. Let $I \subseteq R$ be an ideal of R which is closed under σ, i.e., $p \in I \Rightarrow \sigma(p) \in I$ for all $p \in R$. Show that $I = \{0\}$ or $1 \in I$.

18***.** Let K be a difference field, $\phi \in \mathrm{Const}(K)$ be a primitive mth root of unity and consider the difference ring $R = K[\phi^x]$. For $i = 0, \dots, m-1$, define $g_i = \frac{1}{m}\sum_{j=0}^{m-1} \phi^{ij}(\phi^x)^j$. Show the following facts used in the proof of Theorem 2.29:

a. $R = g_0 K + \cdots + g_{m-1}K$

b. $g_0 + \cdots + g_{m-1} = 1$

c. $g_i^2 = g_i$ for all i and $g_i g_j = 0$ for all $i \neq j$

d. $\sigma(g_i) = g_{i+1}$ for $i = 0, \dots, m-2$ and $\sigma(g_{m-1}) = g_0$

19. Let K be a difference field and $C = \mathrm{Const}(K)$. Let $y_1, \dots, y_r \in K$ and define

$$W(y_1, \dots, y_r) = \begin{vmatrix} y_1 & \cdots & y_r \\ \sigma(y_1) & \cdots & \sigma(y_r) \\ \vdots & & \vdots \\ \sigma^{r-1}(y_1) & \cdots & \sigma^{r-1}(y_r) \end{vmatrix}.$$

Show that $y_1, \dots, y_r$ are linearly dependent over C if and only if $W(y_1, \dots, y_r)=0$.

20. Construct a linear recurrence equation with coefficients in $C(x)$ whose solution space is generated by x, $x!$, and 2^x.

Hint: Apply the criterion of the previous exercise to the desired solutions and an unknown function, and simplify the result.

References

Deformed operators were used by van Hoeij [445] for computing hypergeometric solutions of linear recurrences, as explained in Sect. 2.6. Abramov, Barkatou, van Hoeij, and Petkovšek [25] used them to study the possible dimensions of solution spaces for various kinds of solutions. Our definition of "robust" corresponds to their notion of "subformal". They also consider "submeromorphic", "subanalytic", "subentire" solutions, defined as sequences obtained by restricting meromorphic, analytic, or entire solutions, respectively, to $\mathbb{Z}$. They show that the resulting sequence solutions are the same in all four cases.

A first version of Theorem 2.22 appears in §147 of Nörlund's book on difference calculus [339]. It was generalized by Praagman [360] and Immink [246].

The algebraic perspective using difference rings forms the area of difference algebra, which was introduced in 1965 by Cohn [162] as a discrete analog of differential algebra (cf. Sect. 3.2). Theorem 2.27 appears as Lemma A.5 in a paper of Hendriks and Singer [234]. Theorem 2.29 is a reformulation of Theorem 2.27 that highlights the role of exponential elements in difference rings. They not only cause trouble in the context of D-finite functions but also in the area of symbolic summation [395, 396]. For given algebraic numbers $\phi_1, \dots, \phi_n$, there is an algorithm due to Ge [205] which can find all the algebraic relations among the exponential terms $\phi_1^x, \dots, \phi_n^x$.

2.3 Closure Properties

We have seen in the previous section that the solution set V of a fixed recurrence equation is a C-vector space, i.e., it is closed under taking C-linear combinations. In the present section, we will see more generally that the set of all D-finite sequences is closed under taking C-linear combinations, i.e., even if $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ are two D-finite sequences satisfying distinct recurrence recurrence equations, any linear combination $(\alpha a_n + \beta b_n)_{n=0}^{\infty}$ of them will also satisfy a recurrence equation (usually different from the ones satisfies by $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$).

This property allows us to reduce the question whether two given D-finite sequences are equal to the question of whether a given D-finite sequence is identically zero. For, if $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ are given in terms of recurrences and sufficiently many initial values, then we can compute a recurrence and initial values for $(a_n - b_n)_{n=0}^{\infty}$, and this sequence is identically zero if and only if $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ are equal. Of course we can easily decide whether a given D-finite sequence is identically zero. This is the case if and only if all initial values are zero. As discussed in the previous section, we must not forget to include among the initial values the points where the leading coefficient polynomial vanishes (if there are any).

Theorem 2.30 *(See Theorem 3.25 for the differential case) Let $(a_n)_{n=0}^{\infty} \in C^{\mathbb{N}}$ be D-finite of order r_a and degree d_a and $(b_n)_{n=0}^{\infty} \in C^{\mathbb{N}}$ be D-finite of order r_b and degree d_b.*

1. *$(a_n + b_n)_{n=0}^{\infty}$ is D-finite of order (at most) $r_a + r_b$ and degree (at most) $(r_a + 1)d_b + (r_b + 1)d_a$.*
2. *$(a_n b_n)_{n=0}^{\infty}$ is D-finite of order (at most) $r_a r_b$ and degree (at most) $(r_a r_b + 1)(d_a(r_a(r_b - 1) + 1) + d_b((r_a - 1)r_b + 1))$.* □

Proof Let $p_i, q_i \in C[x]$ be such that

$$p_0(n)a_n + \cdots + p_{r_a}(n)a_{n+r_a} = 0,$$
$$q_0(n)b_n + \cdots + q_{r_b}(n)b_{n+r_b} = 0,$$

for all $n \in \mathbb{N}$. Suppose that p_{r_a} and q_{r_b} are not zero.

1. We are free to replace n by $n + i$ in the given recurrence equations, for any $i \in \mathbb{N}$, and to multiply these equations by polynomials. We will show that there is a recurrence equation which can be reached by these operations from either

of the two given equations. This equation will therefore have $(a_n)_{n=0}^{\infty}$ as well as $(b_n)_{n=0}^{\infty}$ as a solution, and hence also the sum $(a_n + b_n)_{n=0}^{\infty}$.
Make an ansatz

$$\sum_{j=0}^{r_b} u_j(n) \sum_{i=0}^{r_a} p_i(n+j)a_{n+i+j} = 0,$$

$$\sum_{j=0}^{r_a} v_j(n) \sum_{i=0}^{r_b} q_i(n+j)b_{n+i+j} = 0,$$

with unknown polynomial coefficients u_j, v_j. Note that as soon as one of the u_j is nonzero, the first equation is nontrivial, and likewise for the second equation.
Equating the coefficient of a_{n+k} to the coefficient of b_{n+k}, for $k = 0, \dots, r_a + r_b$ gives a linear system with $(r_a + 1) + (r_b + 1)$ variables (the u_j and v_j) and $r_a + r_b + 1$ equations (one for each k). The coefficients of the variables u_j are polynomials of degree at most d_a while the coefficients of the variables v_j are polynomials of degree at most d_b.
This linear system must have a nonzero solution. By Theorem 1.29, there is a solution vector with polynomial entries where the entries corresponding to the variables u_j have degrees bounded by $r_b d_a + (r_a + 1)d_b$ and those corresponding to the variables v_j have degrees bounded by $(r_b + 1)d_a + r_a d_b$.
Taking as u_j and v_j the components of a solution vector, the equations from the ansatz become equal. Furthermore, for a nonzero solution vector, at least one u_j or one v_j must be nonzero, which forces at least one of the equations to be nontrivial (and then, since the equations are equal, both are nontrivial). Taking also the degrees of p_i and q_i into account, we see that these equations have polynomial coefficients of degree at most $(r_a + 1)d_b + (r_b + 1)d_a$, as claimed.

2. Using the recurrence for $(a_n)_{n=0}^{\infty}$, we can express the term $p_{r_a}(n)a_{n+r_a}$ as a $C[n]$-linear combination of $a_n, \dots, a_{n+r_a-1}$ with polynomial coefficients of degree at most d_a. Replacing n by $n + 1$ in the recurrence for $(a_n)_{n=0}^{\infty}$ and multiplying the resulting equation by $p_{r_a}(n)$ gives an equation such that we can express $p_{r_a}(n)p_{r_a}(n+1)a_{n+1+r_a}$ as a $C[n]$-linear combination of $a_n, \dots, a_{n+r_a-1}$ with polynomial coefficients of degree at most $2d_a$. In general, for any $i \in \mathbb{N}$, we can express the term $p_{r_a}(n) \cdots p_{r_a}(n+i)a_{n+i+r_a}$ as a $C[n]$-linear combination of $a_n, \dots, a_{n+r_a-1}$ with polynomial coefficients of degree at most $(i + 1)d_a$.
Likewise, for any $i \in \mathbb{N}$, we can express the term $q_{r_b}(n) \cdots q_{r_b}(n+i)b_{n+i+r_b}$ as a $C[n]$-linear combination of $b_n, \dots, a_{n+r_b-1}$ with polynomial coefficients of degree at most $(i + 1)d_b$.
Make an ansatz with undetermined polynomial coefficients $u_0, \dots, u_{r_a r_b} \in C[n]$ for a recurrence

$$u_0(n)(a_n b_n) + \cdots + u_{r_a r_b}(n)(a_{n+r_a r_b} b_{n+r_a r_b}) = 0.$$

After multiplying this equation by $p_{r_a}(n)\cdots p_{r_a}(n+r_ar_b-r_a)q_{r_b}(n)\cdots q_{r_b}(n+r_ar_b-r_b)$, we can rewrite it as a linear combination of $a_{n+i}b_{n+j}$ ($i=0,\ldots,r_a-1$, $j=0,\ldots,r_b-1$) with polynomial coefficients of degrees at most $(r_a(r_b-1)+1)d_a+(r_b(r_a-1)+1)d_b$ which still depend linearly on the unknown coefficients $u_0,\ldots,u_{r_ar_b}$. Equating these coefficients to zero gives a linear system over $C[n]$ with r_ar_b+1 variables (the unknowns u_i) and r_ar_b equations (one for each of the terms $a_{n+i}b_{n+j}$).

This linear system must have a nonzero solution. By Theorem 1.29, there is a solution vector with polynomial entries of degree at most $r_ar_b((r_a(r_b-1)+1)d_a+(r_b(r_a-1)+1)d_b)$. Taking the components of this vector times $p_{r_a}(n)\cdots p_{r_a}(n+r_ar_b-r_a)q_{r_b}(n)\cdots q_{r_b}(n+r_ar_b-r_b)$ as $u_0,\ldots,u_{r_ar_b}$ gives the desired recurrence for the sum $(a_nb_n)_{n=0}^{\infty}$. ∎

Example 2.31 Let $a_n = n!$ and $b_n = F_n$, the nth Fibonacci number. We have the recurrence equations $a_{n+1}-(n+1)a_n = 0$ and $b_{n+2}-b_{n+1}-b_n = 0$.

1. Define $c_n = a_n + b_n$. We want to find a recurrence for $(c_n)_{n=0}^{\infty}$. For any polynomials u_0, u_1, u_2, v_0, v_1, we have

$$\begin{aligned}u_0(n)(a_{n+1}-(n+1)a_n)+u_1(n)(a_{n+2}-(n+2)a_{n+1})&\\ +u_2(n)(a_{n+3}-(n+3)a_{n+2})&=0,\\ v_0(n)(b_{n+2}-b_{n+1}-b_n)+v_1(n)(b_{n+3}-b_{n+2}-b_{n+1})&=0.\end{aligned}$$

Rearrange these equations to obtain

$$\begin{aligned}&-(n+1)u_0(n)a_n+(u_0(n)-(n+2)u_1(n))a_{n+1}+(u_1(n)-(n+3)u_2(n))a_{n+2}\\ &\qquad+u_2(n)a_{n+3}=0,\\ &-v_0(n)b_n-(v_0(n)+v_1(n))b_{n+1}+(v_0(n)-v_1(n))b_{n+2}+v_1(n)b_{n+3}=0.\end{aligned}$$

We seek a choice of u_0, u_1, u_2, v_0, v_1 for which the coefficients of these two equations match. In order to find such a choice, we can solve the linear system

$$\begin{pmatrix}-(x+1) & 0 & 0 & 1 & 0\\ 1 & -(x+2) & 0 & 1 & 1\\ 0 & 1 & -(x+3) & -1 & 1\\ 0 & 0 & 1 & 0 & -1\end{pmatrix}\begin{pmatrix}u_0\\ u_1\\ u_2\\ v_0\\ v_1\end{pmatrix}=0.$$

As the system has five variables but only four equations, it must have a nontrivial solution. Indeed, the solution space is generated by

$$(-x^2-4x-3,\ -x^2-3x-3,\ x^2+2x,\ -x^3-5x^2-7x-3,\ x^2+2x).$$

Taking the first three components as u_0, u_1, u_2 and the last two as v_0, v_1, we obtain the desired equation whose solution space contains both $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$, and therefore also $(a_n + b_n)_{n=0}^{\infty} = (c_n)_{n=0}^{\infty}$:

$$\begin{aligned}(n+1)(n^2+4n+3)c_n+(n^3+4n^2+5n+3)c_{n+1}-(n^3+6n^2+9n+3)c_{n+2}\\ +(n^2+2n)c_{n+3}=0.\end{aligned}$$

2. Now let $c_n = a_n b_n$. We want to find a recurrence for $(c_n)_{n=0}^{\infty}$. Following the argument in the proof of the theorem, we make an ansatz

$$u_0(n)c_n + u_1(n)c_{n+1} + u_2(n)c_{n+2} = 0$$

for some unknown polynomials u_0, u_1, u_2. We express c_n, c_{n+1}, c_{n+2} in terms of a_n, b_n, b_{n+1} and obtain

$$\begin{aligned}&u_0(n)a_nb_n + u_1(n)(n+1)a_nb_{n+1} + u_2(n)(n+1)(n+2)a_n(b_n+b_{n+1}) = 0,\\ &(u_0(n) + (n+1)(n+2)u_2(n))a_nb_n\\ &\qquad + ((n+1)u_1(n) + (n+1)(n+2)u_2(n))a_nb_{n+1} = 0.\end{aligned}$$

Equating the expressions in front of the terms a_nb_n and a_nb_{n+1} to zero gives the linear system

$$\begin{pmatrix}1 & 0 & (x+1)(x+2)\\ 0 & x+1 & (x+1)(x+2)\end{pmatrix}\begin{pmatrix}u_0\\ u_1\\ u_2\end{pmatrix} = 0.$$

Again the system must have a nontrivial solution because it has more variables than equations. The solution space is generated by $(-2-3x-x^2, -2-x, 1)$. We have thus found the recurrence

$$-(n^2+3n+1)c_n - (n+2)c_{n+1} + c_{n+2} = 0.$$

The example is somewhat degenerate because we could have easily found the recurrence without solving a linear system (see Exercise 10). □

The polynomial coefficients of the recurrence equations constructed in the proof of part 2 of Theorem 2.30 have a large common factor. We have not divided this factor out, because in general it may have roots in the index range $\mathbb{N}$. In such a case, dividing out the factor may lead to a recurrence that is violated at finitely many points. Of course, factors which have no roots in $\mathbb{N}$ can safely be canceled out. In the generic case, where common factors can be canceled out, the degree bound drops to $r_a r_b(d_a(r_a(r_b-1)+1)+d_b((r_a-1)r_b+1))$. The actual degrees appear to still be somewhat smaller (see Exercise 16).

The ansatz used for addition generically produces a recurrence from which no polynomial factors can be canceled. The degree bound for this case is generically tight as stated in the theorem (see Exercise 16). Note however that in specific examples the approach may accidentally produce a recurrence whose coefficients share a common factor. In this case, it is in general not safe to cancel factors with integer roots from the equation.

Theorem 2.30 not only applies to D-finite sequences but works in any difference ring which contains $C[x]$ and where $\deg\sigma(x) \leq 1$. In particular, whenever R is a difference ring containing $C[x]$, then the set of all D-finite elements of R (i.e., all elements of R which satisfy some linear recurrence equation with polynomial coefficients) forms a subring of R. It is also not really essential that the coefficients are polynomials. The proof shows more generally that when a, b are elements of some difference ring R which satisfy linear recurrence equations of respective orders r_a, r_b with coefficients in some difference subfield K of R, then $a+b$ and ab satisfy recurrence equations of respective orders $r_a + r_b$ and $r_a r_b$ with coefficients in K.

The general term *closure properties* refers to operations that preserve D-finiteness. According to Theorem 2.30, the class of D-finite sequences is closed under addition and multiplication. There are some further closure properties for D-finite sequences.

Theorem 2.32 *Let $(a_n)_{n=0}^\infty$ be D-finite of order r and degree d.*

1. *For every $m \in \mathbb{N}$, the sequence $(a_{n+m})_{n=0}^\infty$ is D-finite of order r and degree d.*
2. *$(a_{n+1} - a_n)_{n=0}^\infty$ is D-finite of order (at most) r and degree (at most) $2d$.*
3. *$(\sum_{k=0}^n a_k)_{n=0}^\infty$ is D-finite of order (at most) $r+1$ and degree (at most) d.*
4. *For fixed positive $m \in \mathbb{N}$, define b_n as $a_{n/m}$ if $m \mid n$ and $b_n = 0$ otherwise. Then $(b_n)_{n=0}^\infty$ is D-finite of order (at most) mr and degree (at most) d.*
5. *For every positive $m \in \mathbb{N}$, the recurrence $(a_{\lfloor n/m \rfloor})_{n=0}^\infty$ is D-finite of order (at most) $mr + 1$ and degree (at most) $2d$.*
6. *For every positive $m \in \mathbb{N}$, the sequence $(a_{mn})_{n=0}^\infty$ is D-finite of order (at most) r and degree (at most) $(r+1)d(r(m-1)-1)$.* □

Proof Let $p_0, \ldots, p_r \in C[x]$ be polynomials of degree $\leq d$ such that $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ for all $n \in \mathbb{N}$.

1. We clearly have $p_0(n+m)a_{n+m} + \cdots + p_r(n+m)a_{n+m+r} = 0$ for all $n \in \mathbb{N}$.
2. Using summation by parts, we can write

$$0 = \sum_{i=0}^{r} p_i(n)a_{n+i} = q_r(n)a_n + \sum_{i=0}^{r-1} q_i(n)(a_{n+i+1} - a_{n+i}),$$

with $q_i = p_0 + \cdots + p_i$ $(i = 0, \ldots, r)$. Applying the operator $q_r S - \sigma(q_r)$ to this equation gives

$$q_r(n+1)q_r(n)(a_{n+1} - a_n) + q_r(n)\sum_{i=0}^{r-1} q_i(n+1)(a_{n+i+2} - a_{n+i+1})$$
$$- q_r(n+1)\sum_{i=0}^{r-1} q_i(n)(a_{n+i+1} - a_{n+i}) = 0.$$

This is a recurrence of order $\leq r$ and degree $\leq 2d$ for $(a_{n+1} - a_n)_{n=0}^{\infty}$.

3. Write $s_n = \sum_{k=0}^{n-1} a_k$, so that $s_{n+1} - s_n = a_n$. Then $\sum_{i=0}^{r} p_r(n)(s_{n+1} - s_n) = 0$ is a recurrence for $(s_n)_{n=0}^{\infty}$ of order at most r and degree at most d. According to part 1, the sequence $(s_{n+1})_{n=0}^{\infty}$ has a recurrence of the same shape.
4. We have $b_{nm} = a_n$ for all $n \in \mathbb{N}$. Hence $p_0(n)b_{mn} + \cdots + p_r(n)b_{m(n+r)} = 0$ for all $n \in \mathbb{N}$. Hence $p_0(n/m)b_n + p_1(n/m)b_{n+m} + \cdots + p_r(n/m)b_{n+mr} = 0$ for all $n \in m\mathbb{N}$. For every $i \in \{1, \ldots, m-1\}$ we have $b_n = 0$ for all $n \in m\mathbb{N} + i$. Therefore, the recurrence $p_0(n/m)b_n + p_1(n/m)b_{n+m} + \cdots + p_r(n/m)b_{n+mr} = 0$ holds for all $n \in \mathbb{N}$.
5. Define $b_n = a_{\lfloor (n+1)/m \rfloor} - a_{\lfloor n/m \rfloor}$ for $n \in \mathbb{N}$. Then $b_n = 0$ for all $n \in \mathbb{N}$ with $m \nmid n+1$, and we have $b_n = a_{(n+1)/m} - a_{(n+1)/m-1}$ for all $n \in \mathbb{N}$ with $m \mid n+1$. Note that $m \mid n+1$ implies $\lfloor n/m \rfloor = (n+1)/m - 1$.
By parts 1, 2, and 4, it follows that $(b_n)_{n=0}^{\infty}$ is D-finite of order $\leq mr$ and degree $\leq 2d$.
Now observe that $a_{\lfloor n/m \rfloor} = a_0 + \sum_{k=0}^{n-1} b_k$ for all $n \in \mathbb{N}$, so the claim follows using part 3.
6. For every integer $i \geq r$, the term $p_r(n) \cdots p_r(n+i-r)a_{n+i}$ can be written as a $C[n]$-linear combination of the terms $a_n, \ldots, a_{n+r-1}$ with polynomial coefficients of degree at most $(i - r + 1)d$. Make an ansatz with undetermined polynomial coefficients $u_0, \ldots, u_r \in C[x]$ for a recurrence

$$u_0(n)a_n + u_1(n)a_{n+m} + \cdots + u_r(n)a_{n+rm} = 0.$$

After multiplying this equation by $p_r(n) \cdots p_r(n+r(m-1))$, we can rewrite this equation as a linear combination of $a_n, \ldots, a_{n+r-1}$ with polynomial coefficients of degree at most $d(r(m-1)-1)$ which still depend linearly on the unknown polynomials $u_0, \ldots, u_r$. Equating these coefficients to zero gives a linear system over $C[x]$ with $r+1$ variables (the unknowns u_i) and r equations (one for each of the terms $a_n, \ldots, a_{n+r-1}$).
This linear system must have a nonzero solution. By Theorem 1.29, there is a solution vector with polynomial entries of degree at most $rd(r(m-1)-1)$. Taking the components of this vector times $p_r(n) \cdots p_r(n+r(m-1))$ as $u_0, \ldots, u_r$ gives a recurrence for $(a_n)_{n=0}^{\infty}$ in which all shifts are multiples of m. This recurrence holds for all $n \in \mathbb{N}$, so it continues to hold for all $n \in \mathbb{N}$ when n

is replaced by mn. Because of $a_{mn+mi} = a_{m(n+i)}$, the result is a recurrence for $(a_{mn})_{n=0}^{\infty}$ of order r and the announced degree. ■

Part 2 of the theorem could also be shown by using part 1 and closure under addition, but the direct argument given here gives a better bound on the size of the recurrence.

By combining several operations of the previous theorem, it follows that if $(a_n)_{n=0}^{\infty}$ is D-finite, then for all nonnegative rational numbers u and v, the sequence $(a_{\lfloor un+v\rfloor})_{n=0}^{\infty}$ is D-finite. Furthermore, combining parts 1 and 4 with closure under addition, it follows that the interlacing of any finite number of D-finite sequences is D-finite.

Theorem 2.33 *(See Theorem 3.5 for a converse) Let $(a_n)_{n=0}^{\infty}$ be D-finite of order r and degree d. Then $a(x) = \sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ satisfies a linear differential equation of order (at most) $d+1$ with polynomial coefficients of degree (at most) $d+2r-1$.* □

Proof Let $p_0, \ldots, p_r \in C[x]$ be polynomials of degree $\leq d$ such that

$$p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$$

for all $n \in \mathbb{N}$. Let $p_{i,j} \in C$ be such that $p_i = \sum_{j=0}^{d} p_{i,j}(x+i)^{\underline{j}}$ for $i = 0, \ldots, r$. Then $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}(n+i)^{\underline{j}} a_{n+i} = 0$ for all $n \in \mathbb{N}$. A power series is zero if and only if all of its coefficients are zero. Therefore,

$$\sum_{n=0}^{\infty}\left(\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}(n+i)^{\underline{j}} a_{n+i}\right)x^n = \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}\left(\sum_{n=0}^{\infty} a_{n+i}(n+i)^{\underline{j}} x^n\right) = 0.$$

For every $i, j \in \mathbb{N}$, we have $a^{(j)}(x) = \sum_{n=0}^{\infty} a_n n^{\underline{j}} x^{n-j} = \sum_{n=-i}^{\infty} a_{n+i}(n+i)^{\underline{j}} x^{n+i-j} = q_{i,j}(x) + x^{i-j}\sum_{n=0}^{\infty} a_{n+i}(n+i)^{\underline{j}} x^n$, for some Laurent polynomial $q_{i,j}$ with exponents in the range from $-j$ to $-j+i-1$. The equation above can now be rewritten as

$$\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j} x^{j-i}(a^{(j)}(x) - q_{i,j}(x)) = 0.$$

Multiply by x^r and reverse the order of the outer sum, then move all the parts involving $q_{i,j}$ to the right hand side. This leads to an equation of the form

$$\sum_{i=0}^{r}\sum_{j=0}^{d} p_{r-i,j} x^{j+i} a^{(j)}(x) = Q(x)$$

for a certain polynomial Q of degree at most $r-1$. This is a linear differential equation of order $\leq d$ with polynomial coefficients of degree $\leq r+d$ and a polynomial of degree $\leq r-1$ as the inhomogeneous part. To finally make the equation homogeneous, apply the differential operator $QD_x - Q'$ on both sides. Doing so increases the order of the equation by one and the degree by at most $r-1$. ■

Example 2.34

1. For $a_n = \frac{1}{n!}$ we have $a(x) = \sum_{n=0}^{\infty} a_n x^n = \exp(x)$. Starting from the recurrence equation $(n+1)a_{n+1} - a_n = 0$, which holds for all $n \in \mathbb{N}$, we obtain by multiplying with x^n and summing over all $n \in \mathbb{N}$ the functional equation

$$\sum_{n=0}^{\infty}(n+1)a_{n+1}x^n - a(x) = 0.$$

   The first series is easily recognized to be the derivative $a'(x)$, so we obtain the expected differential equation of $\exp(x)$.
2. Now let $a_n = n!$. The series $a(x) = \sum_{n=0}^{\infty} a_n x^n$ only converges at the point zero. Nevertheless, as a formal power series, it satisfies a differential equation. The recurrence $a_{n+1} - (n+1)a_n = 0$ translates into the functional equation

$$\sum_{n=0}^{\infty} a_{n+1}x^n - \sum_{n=0}^{\infty}(n+1)a_n x^n = 0.$$

   The first series in this equation is $\frac{1}{x}(a(x)-1)$. The second series is $xa'(x)+a(x)$. We thus have the equation

$$a(x) - x^2 a'(x) - xa(x) = 1.$$

   Differentiating in order to eliminate the right hand side gives

$$-x^2 a''(x) - (3x-1)a'(x) - a(x) = 0.$$

□

Theorem 2.33 is a counterpart of Theorem 3.5, which says that every D-finite power series has a D-finite coefficient sequence. Both theorems together allow us to switch back and forth between the two points of view without losing D-finiteness. This enables us to translate closure properties for D-finite power series into additional closure properties for D-finite sequences. For example, the closure of D-finite power series under multiplication (Theorem 3.25) translates into the closure of D-finite sequences under Cauchy product (convolution): if $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ are D-finite, then so is the sequence $(c_n)_{n=0}^{\infty}$ defined by $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ for $n \in \mathbb{N}$. This includes part 3 of Theorem 2.32 as a special case.

For random input, the transformation of recurrence equations to differential equations and back can lead to equations of unreasonably high degree. For example, taking two random recurrence equations of order 2 and degree 2, transforming them to differential equations, then computing a differential equation for the product of the two series, and then converting this differential equation back to a recurrence may lead to one of order 156 and degree 16, even though the convolution also satisfies a recurrence of order 12 and degree 52.

For examples coming from applications, the effect is typically less dramatic, but it is not uncommon that recurrence equations computed by the algorithms behind the proofs of this section may not have minimal possible order. The phenomenon also arises for the closure properties discussed in Theorems 2.30 and 2.32. The reason in these cases is that the algorithms produce recurrences which are valid for any solution of the input recurrences, not just for the particular solution we have in mind. For example, if $(a_n)_{n=0}^{\infty}$ satisfies a certain recurrence of order r and degree d, then the sequence $(-a_n)_{n=0}^{\infty}$ satisfies the very same recurrence, but if we apply the algorithm behind the proof of Theorem 2.30 (part 1) to two times the same recurrence, we won't get the order-0 recurrence satisfied by $(a_n - a_n)_{n=0}^{\infty}$. Instead, the output will be again the recurrence of $(a_n)_{n=0}^{\infty}$. The order of this recurrence is r, which is less than the generic order $2r$, but more than 0. It cannot be less than r though, because the output recurrence must annihilate all sequences $(a'_n + a''_n)_{n=0}^{\infty}$ where $(a'_n)_{n=0}^{\infty}$ and $(a''_n)_{n=0}^{\infty}$ are solutions of the input recurrence.

In applications, it is typically advisable to keep the order of recurrences small. Suppose we have a sequence $(a_n)_{n=0}^{\infty}$ for which we have constructed a recurrence equation that presumably has non-minimal order. We can try to find a recurrence of lower order by guessing (Sect. 1.5). If we succeed, it is not difficult to prove that the guessed equation is correct. Consider the sequence $(b_n)_{n=0}^{\infty}$ defined by the guessed recurrence and the same initial values as $(a_n)_{n=0}^{\infty}$. Then $(b_n)_{n=0}^{\infty}$ satisfies the guessed recurrence by definition. Using the non-minimal recurrence for $(a_n)_{n=0}^{\infty}$ and the defining recurrence for $(b_n)_{n=0}^{\infty}$, we can compute a recurrence for $(a_n - b_n)_{n=0}^{\infty}$ and use it to prove that $a_n = b_n$ for all $n \in \mathbb{N}$. If this works, we can conclude that the guessed recurrence also holds for $(a_n)_{n=0}^{\infty}$. Another possibility is to define b_n as the left hand side of the guessed equation for $(a_n)_{n=0}^{\infty}$ and to use closure properties to compute a recurrence for this sequence $(b_n)_{n=0}^{\infty}$ (see Exercise 6). Then prove that $b_n = 0$ for all $n \in \mathbb{N}$ by checking a sufficient number of initial values.

Either way, if $(a_n)_{n=0}^{\infty}$ was an intermediate result in a longer computation consisting, say, of several applications of algorithms for closure properties, then it is usually preferable to continue the computation with the guessed-and-proved low-order recurrence.

Example 2.35 Let $(a_n)_{n=0}^{\infty}$ be defined by $a_0 = 1$, $a_1 = 2$, $a_2 = 5$, and

$$\begin{aligned} 8(2n+1)(n^2+3n+3)a_n - 4(n+1)(5n^2+13n+9)a_{n+1} \\ + 2(4n^3+15n^2+17n+9)a_{n+2} - (n+3)(n^2+n+1)a_{n+3} = 0 \end{aligned}$$

for $n \in \mathbb{N}$.

1. Using the recurrence, compute the first few terms of the sequence and apply guessing. This may lead to the conjectured recurrence

$$4(n+1)(2n+1)a_n - 2(3n^2+5n+1)a_{n+1} + n(n+2)a_{n+2} \stackrel{?}{=} 0.$$

Define $(b_n)_{n=0}^\infty$ by $b_0 = 1, b_1 = 2$ and this recurrence. By the algorithm behind Theorem 2.30, compute a recurrence for $(b_n - a_n)_{n=0}^\infty$. It turns out that this sequence satisfies the same third order recurrence by which $(a_n)_{n=0}^\infty$ was defined. After checking $b_2 = 5$, it follows that $a_n = b_n$ for all $n \in \mathbb{N}$. Thus, the guessed recurrence was right.
Using the other approach, let $b_n = 4(n+1)(2n+1)a_n - 2(3n^2+5n+1)a_{n+1} + n(n+2)a_{n+2}$ $(n \in \mathbb{N})$ and use algorithms for executing closure properties to find a recurrence equation for $(b_n)_{n=0}^\infty$. It turns out that $(b_n)_{n=0}^\infty$ satisfies the recurrence $(n^2+n+1)b_{n+1} - 2(n^2+3n+3)b_n = 0$ $(n \in \mathbb{N})$. After checking that $b_0 = 0$, it follows that $b_n = 0$ for all $n \in \mathbb{N}$, confirming again that the guessed recurrence for $(a_n)_{n=0}^\infty$ is true.
2. The first few terms of the sequence $(a_n)_{n=0}^\infty$ are also consistent with the recurrence

$$\begin{aligned} &2(662n^4 + 6642n^3 + 1141n^2 + 219081n + 95154)a_n \\ &- (298n^4 + 4617n^3 - 11644n^2 + 169719n + 95154)a_{n+1} \stackrel{?}{=} 0. \end{aligned}$$

Defining $(b_n)_{n=0}^\infty$ via this recurrence and the initial value $b_0 = 1$ and computing a recurrence for $c_n := b_n - a_n$ gives a recurrence of the form

$$(\dots)c_n + (\dots)c_{n+1} + (\dots)c_{n+2} + (\dots)c_{n+3} + (n-6)(n+4)(\dots)c_{n+4} = 0,$$

where the $\dots$ suppress some polynomials that are irrelevant for our purpose. Because of the factor $n-6$, we need to check $c_n \stackrel{?}{=} 0$ for $n = 0, \dots, 10$, and sure enough it turns out that $c_0 = \dots = c_9 = 0 \neq c_{10} = \frac{163926}{125009}$, thus disproving the guessed recurrence.
The other approach leads to the same conclusion. Defining $b_n = 2(662n^4 + 6642n^3 + 1141n^2 + 219081n + 95154)a_n - (298n^4 + 4617n^3 - 11644n^2 + 169719n + 95154)a_{n+1}$ and computing a recurrence for $(b_n)_{n=0}^\infty$ gives a recurrence of the form

$$(\dots)b_n + (\dots)b_{n+1} + (\dots)b_{n+2} + (n-6)(n+4)(\dots)b_{n+3} = 0.$$

In order to prove that $b_n = 0$ for all $n \in \mathbb{N}$, we must check $n = 0, \dots, 9$, and sure enough it turns out that $b_0 = \dots = b_8 = 0 \neq b_9 = 7868448$. □

Exercises

1. Show that $\sum_{k=1}^{\lfloor n/3 \rfloor} \binom{5k+3}{2k+4} \Big(\sum_{i=1}^{2k+3} \frac{3i^2+5i-2}{3i^2+i+1}(2^i + 3^i) \Big)^5$ is D-finite.

2⋆. Show that the binomial coefficient $\binom{\lfloor un+v \rfloor}{\lfloor sn+t \rfloor}$ is D-finite w.r.t. n for all fixed positive rational numbers u, v, s, t.

3⋆. (Ramanujan) Prove the identity $\lfloor \frac{n}{3} \rfloor + \lfloor \frac{n+2}{6} \rfloor + \lfloor \frac{n+4}{6} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n+3}{6} \rfloor$ $(n \in \mathbb{N})$.

4⋆. Prove the identity $\sum_{k=0}^{n} (-\frac{1}{4})^k \binom{n}{k}\binom{2k}{k} = (\frac{1}{4})^n \binom{2n}{n}$ $(n \in \mathbb{N})$.

5. Let $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$, $(c_n)_{n=0}^{\infty}$ be D-finite sequences, and let

$$d_n := \sum_{i,j,k: i+j+k=n} a_i b_j c_k$$

for $n \in \mathbb{N}$. Show that $(d_n)_{n=0}^{\infty}$ is D-finite.

6. (Christoph Koutschan) Let $(a_n)_{n=0}^{\infty}$ be D-finite of order r. Let $p_0, \dots, p_{r-1}$ be polynomials and $b_n = p_0(n)a_n + \cdots + p_{r-1}(n)a_{n+r-1}$ for $n \in \mathbb{N}$. Using Theorems 2.32 and 2.30 and the fact that each p_i satisfies a recurrence of order 1, it follows that $(b_n)_{n=0}^{\infty}$ satisfies a recurrence of order $\le r^2$. Show that it actually satisfies a recurrence of order $\le r$.

7. Let $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ be two sequences. Suppose that $(a_n)_{n=0}^{\infty}$ is D-finite and that there are only finitely many $n \in \mathbb{N}$ with $a_n \ne b_n$. Show that $(b_n)_{n=0}^{\infty}$ is D-finite.

8. Let $(a_n)_{n=0}^{\infty}$ be D-finite of order r. According to Theorem 2.30, the sequence $(a_n^2)_{n=0}^{\infty}$ satisfies a recurrence of order at most r^2. Show that it even satisfies a recurrence of order $\frac{1}{2}r(r+1)$.

9⋆. Let $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$, $(c_n)_{n=0}^{\infty}$ be D-finite of orders r_a, r_b, r_c and degrees d_a, d_b, d_c, respectively. By applying Theorem 2.30 twice, we find that $(a_n + b_n + c_n)_{n=0}^{\infty}$ satisfies a recurrence of order $r_a + r_b + r_c$ and degree $(r_a + r_b + 1)d_c + (r_c + 1)((r_a + 1)d_b + (r_b + 1)d_a)$. Show that the degree bound can be improved to $(r_b + r_c + 1)d_a + (r_a + r_c + 1)d_b + (r_a + r_b + 1)d_c$.

10. Let $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ be sequences satisfying recurrence equations $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ and $q_0(n)b_n - q_1(n)b_{n+1} = 0$ with $p_0, \dots, p_r, q_0, q_1 \in C[x]$ and $q_0, q_1 \ne 0$. Without solving a linear system, determine a recurrence for $(a_n b_n)_{n=0}^{\infty}$.

11⋆. Suppose $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ satisfy the recurrence equations $(1+2n)a_n + (3+4n)a_{n+1} + (5+6n)a_{n+2} = 0$ and $(7+8n)b_n + (9+10n)b_{n+1} + (11+12n)b_{n+2} = 0$, respectively. Compute recurrence equations for the sequences $(a_n + b_n)_{n=0}^{\infty}$ and $(a_n b_n)_{n=0}^{\infty}$.

12. Suppose the sequence $(a_n)_{n=0}^{\infty}$ satisfies the recurrence $(1+2n)a_n + (3+4n)a_{n+1} + (5+6n)a_{n+2} = 0$. Compute a recurrence for $(b_n)_{n=0}^{\infty}$, where **a.** $b_n = a_{n+1}$, **b.** $b_n = a_{2n}$, **c.** $b_n = a_{\lfloor n/2 \rfloor}$, **d.** $b_n = \sum_{k=0}^{n} a_k$.

13. Suppose the sequence $(a_n)_{n=0}^{\infty}$ satisfies the recurrence $(1+2n)a_n + (3+4n)a_{n+1} + (5+6n)a_{n+2} = 0$. Find a differential equation for $a(x) = \sum_{n=0}^{\infty} a_n x^n$.

14***. In the context of Theorem 2.33, show more precisely that the differential equation for $a(x)$ has the form $\sum_{j=0}^{d+1} q_j(x) a^{(j)}(x) = 0$ for polynomials q_j of degree at most $j + 2r - 2$, for $j = 0, \ldots, d+1$.

15*. In the context of Theorem 2.33, show that there is also a differential equation of order $r + d$ and degree $r + d$.

16. For various choices of r_a, r_b, d_a, d_b, define two D-finite sequences $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ via random initial values and random recurrence equations of orders r_a, r_b and degrees d_a, d_b, respectively. Using an efficient guessing program, find recurrence equations for $(a_n + b_n)_{n=0}^{\infty}$ and $(a_n b_n)_{n=0}^{\infty}$ of smallest possible order. Apply multivariate polynomial interpolation (or linear algebra) to construct conjectures about how orders and degrees of these operators depend on r_a, r_b, d_a, d_b. Compare your results to the bounds stated in Theorem 2.30.

17*. Prove or disprove:
- **a.** The sum of two non-D-finite sequences is not D-finite.
- **b.** The product of two non-D-finite sequences is not D-finite.
- **c.** The interlacing of two non-D-finite sequences is not D-finite.
- **d.** If $(a_n)_{n=0}^{\infty}$ is D-finite, then so is $(a_{n^2})_{n=0}^{\infty}$.
- **e.** If $(a_n)_{n=0}^{\infty}$ is D-finite, then so is $(a_{n \bmod 5})_{n=0}^{\infty}$.

18*. Show that the Fibonacci sequence $(F_n)_{n=1}^{\infty}$ is not the interlacing of a finite number of exponential sequences, i.e., sequences of the form $(c\psi^n)_{n=1}^{\infty}$ for some $c, \psi \in C$.

19. The Gamma function satisfies the recurrence $\Gamma(z+1) = z\Gamma(z)$ for all $z \in \mathbb{C}$. Show that the digamma function $\psi(z) := \Gamma'(z)/\Gamma(z)$ also satisfies a recurrence. More generally, show that if a meromorphic function f satisfies a recurrence $f(z+1) = r(z)f(z)$ for some rational function r, then $g(z) := f'(z)/f(z)$ also satisfies a recurrence.

References

See the references given at the end of Sect. 3.3.

2.4 Generalized Series Solutions

It is not meaningful to ask for solutions of a linear recurrence in the ring $C[[x]]$, because the shift operation $f(x) \mapsto f(x+1)$ does not make sense in this ring. The reason is that for $f(x) = \sum_{n=0}^{\infty} c_n x^n \in C[[x]]$ the constant term of

$$f(x+1) = \sum_{n=0}^{\infty} c_n (x+1)^n = \sum_{n=0}^{\infty} c_n \sum_{k=0}^{\infty} \binom{n}{k} x^k = \sum_{k=0}^{\infty} \Bigl(\sum_{n=0}^{\infty} \binom{n}{k} c_n \Bigr) x^k$$

is in general a sum of infinitely many elements of C. In contrast, the shift operation does make sense in the ring $C[[x^{-1}]]$ of formal power series with descending powers of x. To see why this works better, consider a series $f(x) = \sum_{n=0}^{\infty} c_n x^{-n} \in C[[x^{-1}]]$. Then for every $i \in \mathbb{N}$ we have

$$\begin{aligned} f(x+i) &= \sum_{n=0}^{\infty} c_n (x+i)^{-n} = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} c_n \binom{-n}{k} i^k x^{-n-k} \\ &= \sum_{n=0}^{\infty} \sum_{k=n}^{\infty} c_n \binom{-n}{k-n} i^{k-n} x^{-n-(k-n)} = \sum_{k=0}^{\infty} \Bigl(\sum_{n=0}^{k} c_n \binom{-n}{k-n} i^{k-n} \Bigr) x^{-k}. \end{aligned}$$

The coefficient of any term x^{-k} in this series is a linear combination of $c_0, \dots, c_k$, so $f(x+i)$ is a well-defined element of $C[[x^{-1}]]$.

It is meaningful to ask for the solution space of a linear recurrence with polynomial coefficients in $C[[x^{-1}]]$. Whether it is also worthwhile is another question. Indeed, while linear differential equations with polynomial coefficients typically have a full set of solutions in $C[[x]]$, linear recurrences with polynomial coefficients typically do not have any nonzero solutions in $C[[x^{-1}]]$, although they may. The goal of this section is to show that there is always a full set of series solutions of a somewhat more general type. We will show that for an algebraically closed constant field C, any linear recurrence of order r with polynomial coefficients (and with $p_0 \neq 0$ and $p_r \neq 0$) admits r linearly independent solutions of the following form:

$$\overbrace{\boxed{\Gamma(x)^{u/v}}}^{\text{factorial part}}\ \overbrace{\boxed{\phi^x}}^{\text{exponential part}}\ \overbrace{\boxed{\exp\bigl(s_1 x^{1/v} + s_2 x^{2/v} + \cdots + s_{v-1} x^{(v-1)/v}\bigr)}}^{\text{subexponential part}}$$

$$\times \underbrace{\boxed{x^{\alpha}}}_{\text{polynomial part}} \underbrace{\boxed{\Bigl(\bigl(c_{0,0} + c_{0,1} x^{-1/v} + c_{0,2} x^{-2/v} + \cdots\bigr) + \underbrace{\boxed{\begin{aligned} &\bigl(c_{1,0} + c_{1,1} x^{-1/v} + c_{1,2} x^{-2/v} + \cdots\bigr)\log(x) \\ &+ \cdots \\ &+ \bigl(c_{m,0} + c_{m,1} x^{-1/v} + c_{m,2} x^{-2/v} + \cdots\bigr)\log(x)^m \end{aligned}}}_{\text{logarithmic part}} \Bigr)}}_{\text{series part}}$$

In this expression, we have $v \in \mathbb{N} \setminus \{0\}$, $u \in \mathbb{Z}$, $m \in \mathbb{N}$, $\phi, \alpha \in C$, $s_1, \dots, s_{v-1} \in C$, and $c_{i,j} \in C$ for all i, j. We call such an object a *generalized series* and will use the indicated names for its subexpressions. Except for the zero series, we may assume that at least one of the coefficients $c_{0,0}, \dots, c_{m,0}$ is nonzero, and if k is maximal with $c_{k,0} \neq 0$, we call $\Gamma(x)^{u/v}\phi^x \exp(s_1 x^{1/v} + \cdots + s_{v-1}x^{(v-1)/v} \cdots)x^\alpha \log(x)^k$ the *dominant term* of the generalized series.

The shift operation defined through the rules

$$
\begin{aligned}
\Gamma(x+i) &= x^{\bar{i}}\Gamma(x),\\
\phi^{x+i} &= \phi^i \phi^x,\\
(x+i)^\alpha &= \sum_{n=0}^{\infty} \binom{\alpha}{n} i^n x^{\alpha-n},\\
\exp(s_\ell(x+i)^{\ell/v}) &= \exp(s_\ell x^{\ell/v}) \exp(s_\ell((x+i)^{\ell/v} - x^{\ell/v}))\\
&= \exp(s_\ell x^{\ell/v}) \sum_{n=0}^{\infty} \frac{1}{n!}\left(s_\ell \sum_{k=1}^{\infty} \binom{\ell/v}{k} i^k x^{\ell/v-k}\right)^n,\\
\log(x+i) &= \log(x) + \log\left(1 + \frac{i}{x}\right) = \log(x) - \sum_{n=1}^{\infty} \frac{(-i)^n}{n} x^{-n}
\end{aligned}
$$

maps any generalized series to another generalized series with the same $u, v, m, \phi, \alpha, s_1, \dots, s_{v-1}$. Also a $C[x]$-linear combination of some generalized series with the same $u, v, m, \phi, \alpha, s_1, \dots, s_{v-1}$ is again a generalized series. It is therefore meaningful to ask for generalized series solutions of a given recurrence. It is also worthwhile to find such solutions, because they can provide valuable information about the asymptotic behavior of sequence solutions.

Example 2.36

1. The recurrence

$$
\begin{aligned}
&8(2x+1)^2(2x+3)(3x+4)f(x) + 2(x+1)(2x+3)(15x^2+29x+10)f(x+1)\\
&\quad + (x+1)(3x+1)(x+2)^2 f(x+2) = 0
\end{aligned}
$$

has the following two generalized series solutions:

$$
\begin{aligned}
&(-16)^x x^{-1}\left(1 - \tfrac{1}{4}x^{-1} + \tfrac{1}{32}x^{-2} + \tfrac{1}{128}x^{-3} + \cdots\right),\\
&(-4)^x x^{-1/2}\left(1 - \tfrac{1}{8}x^{-1} + \tfrac{1}{128}x^{-2} + \tfrac{5}{1024}x^{-3} + \cdots\right).
\end{aligned}
$$

Reading them as asymptotic expansions, the first series dominates the second. Therefore, we can expect that almost every sequence solution of the recurrence has an asymptotic expansion which can be described by a constant multiple of the first series. For example, consider the sequence solution defined by the initial values $f(0) = 1$, $f(1) = 0$, and consider the truncation

$$g(x) := (-16)^x x^{-1}\Big(1 - \tfrac{1}{4}x^{-1} + \tfrac{1}{32}x^{-2} + \tfrac{1}{128}x^{-3}\Big)$$

of one of the two generalized series solutions. Then we have

$$\begin{aligned} g(10)/f(10) &\approx -3.1416275355158662226,\\ g(100)/f(100) &\approx -3.1415926536675658933,\\ g(1000)/f(1000) &\approx -3.1415926536675658933,\\ g(10000)/f(10000) &\approx -3.1415926535897932392. \end{aligned}$$

The quotients seem to converge to a limit which is suspiciously close to $-\pi$. It is fair to conjecture that $f(n) \sim -\frac{1}{\pi}(-16)^n n^{-1}$ $(n \to \infty)$.
If we include more terms of the expansion in the truncation $g(x)$, the convergence becomes stronger, but we may need to go to larger values of n before it takes effect. If we use the a truncated version of the other generalized series solution, the quotient $f(n)/g(n)$ tends to zero.

2. The recurrence

$$\begin{aligned} &2(2x+1)(4x+1)(4x+3)f(x) - (x+1)(32x^2+64x+39)f(x+1)\\ &\quad + 2(x+1)(x+2)(2x+3)f(x+2) = 0 \end{aligned}$$

has the following two generalized series solutions:

$$\begin{aligned} &4^x x^{-1/2}\Big(1 - \tfrac{1}{24}x^{-1} - \tfrac{5}{6144}x^{-3} + \cdots\Big),\\ &4^x x^{-3/2}\Big(1 - \tfrac{3}{32}x^{-1} - \tfrac{35}{512}x^{-2} + \tfrac{315}{32768}x^{-3} + \cdots\Big). \end{aligned}$$

Also in this case, the first series dominates the second, but this time the dominance is much weaker because the exponential parts agree. As a consequence, we need to take both series into account if we wish to determine the multiplicative constant in the asymptotic expansion of a particular sequence solution. As an example, consider the sequence solution with initial values $f(0) = f(1) = 1$. Write $g(x)$ and $h(x)$ for the truncated series as quoted above (with "$\cdots$" replaced by "0"), and make an ansatz $f(n) \approx \kappa_1 g(n) + \kappa_2 h(n)$ for unknown κ_1, κ_2. Divide by $f(n)$ on both sides and set n to some large values, e.g., $n = 1000, 1500$. This leads to the linear system

$$1 \approx 4.2785257108346316216\kappa_1 + 0.0042783025692235596604\kappa_2,$$

$$1 \approx 4.2787111598685801937\kappa_1 + 0.0028523749729306319045\kappa_2,$$

which can be solved numerically. We find the solution

$$(\kappa_1, \kappa_2) = (0.23369497725510901491, 0.030393203612345617039).$$

As the value of κ_1 is very close to $(\sqrt{2}-1)/\sqrt{\pi}$, we may be willing to conjecture that $f(n) \sim \frac{\sqrt{\pi}}{\sqrt{2}-1} 4^n n^{-1/2}$ $(n \to \infty)$. □

Although asymptotic expansions of D-finite sequences are the primary application of generalized series, we view generalized series as purely algebraic objects that carry no analytic meaning. They generalize the concept of formal power series as introduced in Sect. 1.1. In particular, the series part of a generalized series need not be convergent, and the symbols Γ and exp are not meant to refer to the gamma function and the exponential function, respectively, but have a formal nature similar to that of x in $C[[x]]$ (cf. again Sect. 1.1). The reason why we write them as introduced above, rather than using some additional neutral symbols $y, z, \ldots$, is that this makes it somewhat easier to memorize how the shift operation is defined. Besides this definition, we shall also adopt the relations $\exp(p+q) = \exp(p)\exp(q)$ and $x^{\alpha+\beta} = x^\alpha x^\beta$. Moreover, if ϕ is a kth root of unity, we impose the relation $(\phi^x)^k = 1$. We also use the alternative notation e^p for $\exp(p)$.

The computation of generalized series solutions can be divided into several steps. An implementation will first determine the possible values u/v for the factorial part, then for each of them the possible values ϕ for the exponential part, then for each pair $(u/v, \phi)$ the possible choices $s_1, \ldots, s_{v-1}$ for the subexponential part, and finally for each choice of $(u/v, \phi, s_1, \ldots, s_{v-1})$ the polynomial part and the series part, which together can be viewed as elements of the set $\bigcup_{\alpha \in C} x^\alpha C[[x^{-1/v}]][\log(x)]$. In our discussion, we will start with the last step. Afterwards we will see that the other data is found by applying certain substitutions to the recurrence in order to bring it into a form where solutions in $\bigcup_{\alpha \in C} x^\alpha C[[x^{-1/v}]][\log(x)]$ exist.

Some of the required transformations map the original linear recurrence with polynomial coefficients into a linear recurrence whose coefficients are series with fractional exponents. We will therefore consider the more general setting from the beginning. Given $p_0, \ldots, p_r \in C[[x^{-1/v}]]$ with $p_0, p_r \neq 0$, we want to determine all generalized series $f(x)$ such that

$$p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0.$$

By multiplying the equation with a suitable power of x, we can always assume that $[x^0]p_i \neq 0$ for at least one i, and we will do so. For the infinite series $p_0, \ldots, p_r$ to be "given" means that for any specific $j \in \mathbb{N}$ we know how to determine the coefficients of $x^{-j/v}$ in these series. Write $p_i = \sum_{j=0}^{\infty} p_{i,j} x^{-j/v}$ for the coefficients of the recurrence, and consider a series $f(x) = \sum_{n=0}^{\infty} c_n x^{-n/v}$.

Substituting $f(x)$ into the left hand side of the recurrence, we get another series belonging to $C[[x^{-1/v}]]$, and $f(x)$ is a solution of the recurrence if and only if all coefficients of that other series are zero. A straightforward but somewhat tedious calculation (Exercise 1) confirms that the coefficient of any specific term $x^{-n/v}$ in this series is

$$\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}[x^{-(n+j)/v}]f(x+i) = \sum_{j=0}^{n} c_{n-j} \sum_{k=0}^{\lfloor j/v\rfloor} \binom{-(n-j)/v}{k} \sum_{i=0}^{r} p_{i,j-vk} i^k.$$

The expression on the right can be read as a linear combination of $c_n, c_{n-1}, \dots, c_0$, and since all of these expressions must be zero when $f(x)$ is a solution, it should allow us to compute any coefficient c_n from the earlier coefficients $c_{n-1}, \dots, c_0$. The coefficient of c_n in the equation is $\sum_{i=0}^{r} p_{i,0}$, so c_n is uniquely determined by the earlier coefficients if the value of this sum is nonzero. However, this is too much to ask for. In fact, if $\sum_{i=0}^{r} p_{i,0} \neq 0$, then the only solution in $C[[x^{-1/v}]]$ is the zero series, because there is no chance for some c_n to be the first nonzero coefficient: $c_0 = c_1 = \cdots = c_{n-1} = 0$ then implies $c_n = 0$ for all $n \in \mathbb{N}$. So we better assume that $\sum_{i=0}^{r} p_{i,0} = 0$. Then the expression above is a linear combination of $c_{n-1}, \dots, c_0$ and we can hope to be able to compute c_{n-1} from $c_{n-2}, \dots, c_0$. For every fixed j, the coefficient of c_{n-j} is a polynomial expression in n of degree at most j. If j is a multiple of v, then the coefficient of n^j in this polynomial expression is a nonzero constant multiple of $\sum_{i=0}^{r} p_{i,0} i^{j/v}$, and this sum may or may not be zero. However, because of the Vandermonde determinant, not all of these sums can be zero. Therefore, there is some finite j and a nonzero polynomial η such that for all $n \geq j$ we have $\eta(n-j)c_{n-j} = \cdots$ with a right hand side that is a linear combination of $c_0, \dots, c_{n-j-1}$.

Definition 2.37 Let $p_0, \dots, p_r \in C[[x^{-1/v}]]$ be such that $[x^0]p_i \neq 0$ for at least one i. Let $p_{i,j} \in C$ be such that $p_i = \sum_{j=0}^{\infty} p_{i,j} x^{-j/v}$ for $i = 0, \dots, r$. Consider the recurrence

$$p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0.$$

1. $\chi := p_{0,0} + p_{1,0}x + \cdots + p_{r,0}x^r \in C[x]$ is called the *characteristic polynomial* of the recurrence.
2. If $j \in \mathbb{N}$ is minimal such that $\eta := \sum_{k=0}^{\lfloor j/v\rfloor} \binom{-x/v}{k} \sum_{i=0}^{r} p_{i,j-vk} i^k \in C[x]$ is not the zero polynomial, then η is called the *indicial polynomial* of the recurrence. □

With the terminology introduced in Definition 2.37, the results of the preceding discussion can be summarized as follows:

- If $x-1$ does not divide the characteristic polynomial χ, then the recurrence at hand has no nonzero solutions in $C[[x^{-1/v}]]$.
- The indicial polynomial η is never the zero polynomial and its degree cannot exceed the multiplicity of $x-1$ in the characteristic polynomial.

- If $f(x) = \sum_{n=0}^{\infty} c_n x^{-n/v} \in C[[x^{-1/v}]]$ is a solution of the recurrence, then for every $n \in \mathbb{N}$ we have an equation of the form $\eta(n)c_n = \ldots$, where the right hand side is a linear combination of $c_0, \ldots, c_{n-1}$.

Since η is not the zero polynomial, there exists some $N \in \mathbb{N}$ such that $\eta(n) \neq 0$ for all $n > N$. Therefore, every truncated solution where we know all of the coefficients c_n with $n \leq N$ can be uniquely extended to an infinite series solution. In order to identify a particular solution, we can stop the expansion at the largest integer root of the indicial polynomial.

The indicial polynomial also tells us the possible starting indices of a solution: if the solution $f(x) = \sum_{n=-\infty}^{\infty} c_n x^{-n/v}$ has the starting index $n_0 \in \mathbb{Z}$, i.e., $c_{n_0} \neq 0$ and $c_n = 0$ for all $n < n_0$, then, since $\eta(n_0)c_{n_0}$ is equal to a linear combination of $c_0, \ldots, c_{n_0-1}$, all of which are zero, it follows that n_0 must be a root of η. On the other hand, not every root of the indicial polynomial necessarily gives rise to a series solution. The phenomenon is the same as for sequence solutions of recurrences discussed in Sect. 2.2: a candidate solution which is "born" at a certain root of the indicial polynomial may lead to a contradiction at one of the subsequent roots and "die" there.

Example 2.38

1. For the recurrence

$$(x-3)^3(3x^2+3x-11)f(x) - 2(x-2)^3(3x^2-11)f(x+1)$$
$$+ (x-1)^3(3x^2-3x-11)f(x+2) = 0$$

we have $\chi = (x-1)^2$ and $\eta = 3x(x+3)$. The integer roots -3 and 0 of η correspond to series solutions starting with

$$x^{-3} + 9x^{-4} + 54x^{-5} + \cdots \quad \text{and} \quad 1 + 6x^{-1} + 18x^{-2} + \cdots,$$

respectively.

2. For the recurrence

$$(3x^3 - 24x^2 + 43x + 99)f(x) - 2(3x^3 - 18x^2 + 25x + 42)f(x+1)$$
$$+ (3x^3 - 12x^2 + 7x + 21)f(x+2) = 0$$

we have $\chi = (x-1)^2$ and $\eta = 3x(x+3)$. Although η has two distinct integer roots, its solution space in $C[[x^{-1}]]$ has dimension 1. It is generated by

$$x^{-3} + 9x^{-4} + \tfrac{246}{5}x^{-5} + \cdots.$$

There is no solution which starts with x^0, because if we try to construct such a solution, we get $x^0 + 6x^{-1} + 42x^{-2}$, and the attempt to compute the next term leads to a division by zero.

3. For the recurrence

$$(x+1)f(x) - (2x+3)f(x+1) + (x+2)f(x+2) = 0$$

we have $\chi = (x-1)^2$ and $\eta = x^2$. As η has only one integer root, the solution space of the recurrence in $C[[x^{-1}]]$ must have dimension 1. Indeed, the solution space is generated by the constant solution 1. □

As we have also seen in Sect. 2.2, trouble related to integer roots of the leading coefficient of a recurrence can be avoided by deforming the recurrence. We obtain deformed equations for the coefficient sequence if we start out by looking for solutions of the form $\sum_{n=0}^{\infty} c_n x^{-(n+q)/v}$. The indicial polynomial is then $\eta(x+q)$ and does not have any integer roots if q is understood to be transcendental over C. But if there are no integer roots, there cannot be any series solutions, because no $n \in \mathbb{N}$ qualifies as a starting index.

If we arbitrarily take $c_0 = 1$ as an initial value, then the deformed recurrence will uniquely determine all subsequent coefficients $c_1, c_2, \ldots \in C(q)$ in such a way that the infinite sequence $(c_n)_{n=0}^{\infty} \in C(q)^{\mathbb{N}}$ satisfies the recurrence for all $n \in \mathbb{N} \setminus \{0\}$ and only violates it for $n = 0$. This means that when we plug the series $f(x) = \sum_{n=0}^{\infty} c_n x^{-(n+q)/v}$ into the original recurrence, all terms will cancel, except for the isolated term $\eta(q)x^{-(q+j)/v}$, where j is as in the definition of η. A solution is obtained if we can set q to a root $\alpha \in \mathbb{Z}$ of the indicial polynomial. Also for non-integer roots α we obtain solutions if setting q to α is legitimate for all coefficients $c_n \in C(q)$ $(n \in \mathbb{Z})$. We then get generalized series belonging to $\bigcup_{\alpha \in C} x^{-\alpha/v} C[[x^{-1/v}]]$.

In order to ensure that we get a solution, we have to ensure that setting q to a root of the indicial polynomial does not lead to a division by zero in one of the coefficients $c_n \in C(q)$. A division by zero happens if for some index n the denominator of c_n vanishes. We can predict rather precisely what the possible denominators are. As in Sect. 2.2, the recursive equations for the coefficients c_n imply that for all $n \in \mathbb{N}$, the denominator of c_n divides $\eta(q+1)\cdots\eta(q+n)$. Since η is a polynomial, it follows that for every $\alpha \in C$ there exist only finitely many $k \in \mathbb{Z}$ such that $q - \alpha \mid \eta(q+k)$. Therefore, there exists a finite $e \in \mathbb{N}$ such that $(q-\alpha)^e c_n \in C(q)$ can be evaluated at $q = \alpha$ for every n. If we wish to set q to a certain α, we can ensure that this substitution is legitimate by taking the initial value $c_0 = (q-\alpha)^e$ instead of the initial value $c_0 = 1$, for a suitable choice of e.

Taking this initial value c_0, we find that substituting the series

$$f(x) = \sum_{n=0}^{\infty} c_n x^{-(n+q)/v}$$

into the recurrence yields the term $\eta(q)c_0x^{-(q+j)/v}$. We can now find one solution by setting $q = \alpha$. If α is a multiple root of $\eta(q)c_0$, then we can find further solutions by differentiating with respect to q, because then α is also a root of $\frac{d}{dq}\big(\eta(q)c_0\big)$, and this is the term we obtain by plugging $\frac{d}{dq}f(x)$ into the recurrence. Note that because of $\frac{d}{dq}x^{-(n+q)/v} = -\frac{1}{v}x^{-(n+q)/v}\log(x)$, the solution $\frac{d}{dq}f(x)|_{q=\alpha}$ belongs to $\bigcup_{\alpha\in C} x^{-\alpha/v}C[[x^{-1/v}]][\log(x)]$. If α is a root of $\eta(q)c_0$ of multiplicity m, we can obtain a set of m linearly independent solutions $\frac{d^i}{dq^i}f(x)|_{q=\alpha}$ $(i = 0, \dots, m-1)$. All of these solutions belong to $\bigcup_{\alpha\in C} x^{-\alpha/v}C[[x^{-1/v}]][\log(x)]$. As it is somewhat inconvenient that this infinite union is not a vector space (note that it is not closed under addition), let us introduce the following notation.

Definition 2.39 The set of all C-linear combinations of elements of

$$\bigcup_{\alpha\in C} x^{\alpha}C[[x]][\log(x)]$$

is denoted by $C[[[x]]]$. □

Note that $C[[[x]]]$ is not only a vector space but even an integral domain (Exercise 10). If C is algebraically closed, the construction described above and summarized in the algorithm below finds a basis of the solution space in $C[[[x^{-1/v}]]]$.

Algorithm 2.40 *(See Algorithm 3.37 for the differential case)*
Input: $p_0, \dots, p_r \in C[[x^{-1/v}]]$ *with* $[x^0]p_i \neq 0$ *for at least one* $i \in \{0, \dots, n\}$.
Output: $\deg \eta$ *many linearly independent solutions in* $C[[[x^{-1/v}]]]$ *of the recurrence* $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = 0$, *where* η *is the indicial polynomial of the recurrence. Each basis element is returned as a truncated series that admits a unique extension to a series solution.*

Set $j = -1$ *and* $\eta = 0$.
while $\eta = 0$, *do*
  Set $j = j+1$ *and* $\eta = \sum_{k=0}^{\lfloor j/v\rfloor}\binom{-x/v}{k}\sum_{i=0}^{r}([x^{j-vk}]p_i)i^k \in C[x]$.
Take $N \in \mathbb{N}$ *such that for any two roots* $\alpha, \beta \in C$ *of* η *with* $\alpha - \beta \in \mathbb{Z}$ *we have* $N > |\alpha - \beta|$.
Set $c_0 = 1$ *and recursively compute* $c_1, \dots, c_N \in C(q)$ *such that for* $f(x) = \sum_{n=0}^{N} c_n x^{-(n+q)/v}$ *we have* $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = \eta(q)x^{-(q+j)/v} + \mathrm{O}(x^{-(q+N+j)/v})$.
Initialize $B = \emptyset$.
for all roots $\alpha \in C$ *of* η, *do*
  Let k *be the multiplicity of* $x - \alpha$ *in* η.
  Find the smallest $e \in \mathbb{N}$ *such that* $q - \alpha$ *does not divide the denominator of* $(q-\alpha)^e c_n$ *for any* $n = 0, \dots, N$.
  Set $B = B \cup \big\{\big[\frac{d^i}{dq^i}(q-\alpha)^e f(x)\big]_{q=\alpha} : i = e, \dots, k+e-1\big\}$.
Return B.

Theorem 2.41 *(See Theorem 3.38 for the differential case) Algorithm 2.40 is correct. In particular:*

1. *If C is algebraically closed and ℓ is the degree of the indicial polynomial, the dimension of the solution space in $C[[[x^{-1/v}]]]$ is at least ℓ.*
2. *If the indicial polynomial has a root of multiplicity k, then there is a solution involving logarithmic terms of degree at least $k-1$.*
3. *If the algorithm finds a solution involving logarithmic terms of degree d, then the indicial polynomial has certain roots $\alpha_1, \dots, \alpha_m \in C$ with respective multiplicities $k_1, \dots, k_m \in \mathbb{N}$ such that $k_1 + \dots + k_m > d$ and $\alpha_i - \alpha_j \in \mathbb{Z}$ for all i, j.* □

Proof First, because of the property of N ensured by line 4, every truncated series returned by the algorithm can be uniquely continued to a series solution. Therefore, every element of B indeed corresponds to a solution. Secondly, B is linearly independent, because every series in B starts with a different term $x^\alpha \log(x)^i$, and these terms are linearly independent. This completes the correctness proof.

1. This claim follows from the fact that line 10 supplies k new solutions for every root α of multiplicity k. If C is algebraically closed, then the sum of the multiplicities of the roots of η is equal to the degree of η.
2. This claim also follows from line 10, because we always have $e \geq 0$, and $[\frac{d^i}{dq^i}(q-\alpha)^e f(x)]_{q=\alpha}$ contains the nonzero term $i^{\underline{e}} x^{-(\alpha-j)/v} \log(x)^i$ for some $j \in \mathbb{N}$.
3. Because of line 10, a logarithmic term of degree m can only appear if $m \leq k+e$ for the values of k, e in some iteration of the main loop. Because of the recurrence for the coefficients c_n, the multiplicity of $q-\alpha$ in the denominator of some term c_n can exceed the multiplicity of $q-\alpha$ in the denominator of c_{n+1} by at most the multiplicity of $q+n-\alpha$ in η, for every $n \in \mathbb{N}$. Taking into account that $q-\alpha$ has multiplicity zero in the denominator of $c_0 = 1$, it follows that the number e determined in line 9 will be such that $k+e \leq k_1 + \dots + k_m$. The claim follows. ■

Example 2.42 For the second recurrence in Example 2.38, Algorithm 2.40 finds the second solution

$$\left(1 + 6x^{-1} + 42x^{-2} - \tfrac{4780}{3}x^{-4} + \cdots\right) + \left(\tfrac{244}{3}x^{-3} + 732x^{-4} + \cdots\right)\log(x).$$

For the third recurrence in Example 2.38, Algorithm 2.40 finds the second solution

$$\log(x) + \tfrac{1}{2}x^{-1} - \tfrac{1}{12}x^{-2} + \tfrac{1}{120}x^{-4} - \tfrac{1}{252}x^{-6} + \tfrac{1}{240}x^{-8} + \cdots.$$

□

With Algorithm 2.40 we can determine $\deg \eta$ many linearly independent series solutions. In the examples above, $\deg \eta$ is equal to the multiplicity of $x-1$ in the characteristic polynomial. The degree cannot be larger, but it may be smaller. In this case, there are solutions with nontrivial subexponential parts. As we will see next, taking into account subexponential parts will always allow us to identify ℓ linearly independent solutions, where ℓ is the multiplicity of $x-1$ in the characteristic polynomial of the recurrence under consideration. In order to see under which circumstances the degree of η may be smaller than the multiplicity ℓ, it is more convenient to express the given recurrence in terms of forward differences rather than in terms of shifts. The recurrence

$$p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0$$

can be written in operator notation as

$$\bigl(p_0(x) + p_1(x)S + \cdots + p_r(x)S^r\bigr) \cdot f(x) = 0.$$

The forward difference operator is $\Delta := S - 1$, it maps $f(x)$ to $f(x+1) - f(x)$. Setting $S = \Delta + 1$ in the operator and expanding the powers of $(\Delta + 1)$ using the binomial theorem, we obtain the equivalent formulation

$$\bigl(q_0(x) + q_1(x)\Delta + \cdots + q_r(x)\Delta^r\bigr) \cdot f(x) = 0,$$

with $q_i(x) = \sum_{k=i}^{r} \binom{k}{i} p_k(x)$ for $i = 0, \ldots, r$.

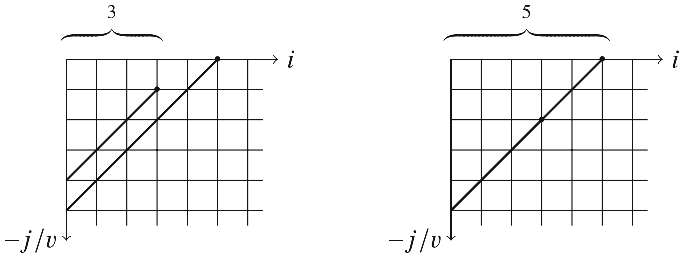
Write the operator in the form $L = \sum_{i=0}^{r} \sum_{j=0}^{\infty} q_{i,j} x^{-j/v} \Delta^i$, where, as before, we may assume that at least one of the $q_{i,0}$ $(i = 0, \ldots, r)$ is nonzero. Observe that the smallest ℓ with $q_{\ell,0} \neq 0$ is precisely the multiplicity of $x-1$ in the characteristic polynomial χ, because $(x-1)^\ell$ divides $\sum_{i=0}^{r} p_{i,0} x^i$ if and only if x^ℓ divides $\sum_{i=0}^{r} p_{i,0}(x+1)^i = \sum_{i=0}^{r} q_{i,0} x^i$.

In order to have a series solution $f(x) = x^\alpha + \cdots$ for the operator L, it is necessary that L annihilates all of the terms of the series, including in particular the dominant term. Because of the relation $\Delta^i \cdot x^\alpha = \alpha^{\underline{i}} x^{\alpha - i} + \cdots$, which holds for every $\alpha \in C$ and every $i \in \mathbb{N}$, equating the dominant term of

$$L \cdot (x^\alpha + \cdots) = \sum_{i=0}^{r} \sum_{j=0}^{\infty} q_{i,j} x^{-j/v} (\alpha^{\underline{i}} x^{\alpha - i} + \cdots)$$

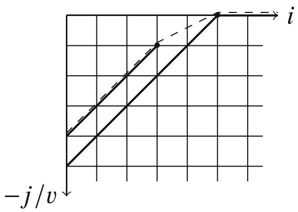
to zero gives a nontrivial polynomial equation for α. This polynomial is exactly the indicial polynomial (with α in place of $-\alpha/v$; cf. Exercise 13). The degree of the indicial polynomial can be read from a diagram: for every $(i, j) \in \mathbb{N}^2$ with $q_{i,j} \neq 0$, draw a diagonal halfline from $(i, -j/v)$ towards south-west, so that it meets the vertical axis at the point $(0, -i - j/v)$. Because of $p_{i,j} x^{-j/v} \Delta^i \cdot (x^\alpha + \cdots) = p_{i,j} \alpha^{\underline{i}} x^{\alpha - i - j/v} + \cdots$, each term $p_{i,j} x^{-j/v} \Delta^i$ of the operator contributes a monomial $p_{i,j} \alpha^{\underline{i}}$ to the coefficient of $x^{\alpha - i - j/v}$ in the resulting series. The indicial polynomial is therefore formed by the terms $p_{i,j} x^{-j/v} \Delta^i$ which correspond to the top-most line segment in the diagram. Its width (meaning the horizontal distance between the vertical axis and the starting point of the segment) is the degree of the indicial polynomial.

Example 2.43 The figures below show the diagrams for the operators $x^{-1}\Delta^3 - \Delta^5$ (left) and $x^{-2}\Delta^3 - \Delta^5$ (right). Their indicial polynomials are $\binom{-x/v}{3}$ and $\binom{-x/v}{3} - \binom{-x/v}{5}$, respectively.



□

Add to the diagram a horizontal halfline from $(\ell, 0)$ towards east, where ℓ is the multiplicity of $x - 1$ in the characteristic polynomial, and consider the convex hull of the set of all the halflines in the diagram. The boundary of this convex hull is called the *Newton polygon* of the operator. For example, the Newton polygon for the operator $x^{-1}\Delta^3 - \Delta^5$ from the example above is the dashed polygon in the following figure:



As we have seen in the example above, solutions in $C[[[x^{-1/v}]]]$ originate from a segment with slope 1. If there are no other segments, as is the case for the second operator in Example 2.43, then we obtain a full set of ℓ linearly independent solutions. Otherwise, if there are further segments, it is clear that they must have a smaller slope. An example is the segment of slope 1/2 in the diagram for the first operator in Example 2.43. We will show that these segments correspond to solutions which have a subexponential part.

Given the operator $L = \sum_{i=0}^{r} \sum_{j=0}^{\infty} q_{i,j} x^{-j/v} \Delta^i$, our goal is to find solutions $f(x)$ that may have a nontrivial subexponential part. The subexponential part is a product of finitely many terms of the form e^{sx^c}, where s is a nonzero constant in C and c is a rational number with $0 < c < 1$. Let $f(x)$ be a solution of L, and write $f(x) = \mathrm{e}^{sx^c} g(x)$, where the subexponential part of $g(x)$ (if there is one) may only have terms $\mathrm{e}^{\tilde{s}x^{\tilde{c}}}$ with $\tilde{s} \in C$ and $\tilde{c} < c$. From the given operator L for $f(x)$, we will extract possible values for s and c, and then for each eligible choice (s, c) construct an operator for $g(x)$ which can then be solved recursively.

In order to recognize the possible values for s and c, consider the action of $\Delta = S - 1$ on a term $x^\alpha e^{sx^c}$. By the discrete version of the product rule, $\Delta(a(x)b(x)) = \Delta(a(x))b(x) + a(x+1)\Delta(b(x))$, we have

$$\begin{aligned}\Delta \cdot (x^\alpha e^{sx^c}) &= (\Delta \cdot x^\alpha)e^{sx^c} + (x+1)^\alpha(\Delta \cdot e^{sx^c})\\ &= (\alpha x^{\alpha-1} + \cdots)e^{sx^c} + (x+1)^\alpha e^{sx^c}\underbrace{e^{s((x+1)^c - x^c)}}_{=scx^{c-1}+\cdots}\\ &= ((sc)x^{\alpha+c-1} + \cdots)e^{sx^c}.\end{aligned}$$

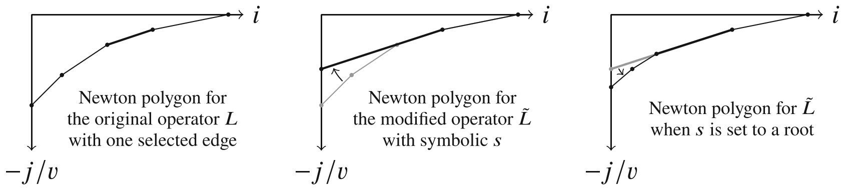
Note for the last step that $x^{\alpha-1}$ is dominated by $x^{\alpha+c-1}$, because we only care about $c > 0$. Repeated application of the argument yields $\Delta^i \cdot (x^\alpha e^{sx^c}) = ((sc)^i x^{\alpha+i(c-1)} + \cdots)e^{sx^c}$, for every $i \in \mathbb{N}$. Therefore, a term $q_{i,j}x^{-j/v}\Delta^i$ of the operator applied to a term e^{sx^c} gives a contribution of $q_{i,j}(sc)^i$ to the coefficient of $x^{-j/v+i(c-1)}e^{sx^c}$ in the resulting series. If there is only one such contribution, it can only vanish if $s = 0$, which means that the term e^{sx^c} is 1 and need not be considered. If there are two distinct terms $x^{-j/v}\Delta^i$ and $x^{-j'/v}\Delta^{i'}$ which contribute to the same term, then this means $-j/v+i(c-1) = -j'/v+i'(c-1)$, so $1-c = \frac{(-j'/v)-(-j/v)}{i'-i}$. So all of the relevant terms of the operator belong to a line of slope $1 - c$ in the diagram considered before. In particular, the terms contributing to the dominant terms of the resulting series belong to the topmost lines with these slopes. These appear as segments of the Newton polygon.

Example 2.44 For the operator $L = x^{-1}\Delta^3 - \Delta^5$ whose diagram is shown in the previous example on the left, the convex hull has an edge of slope $1/2$, which indicates possible solutions involving a subexponential term $e^{sx^{1/2}}$, because $1 - c = 1/2 \Rightarrow c = 1/2$. □

Observe also that edges with slope 1 predict subexponential terms e^{sx^0}, which are constant and can therefore be ignored. This is consistent with our earlier discussion where we saw that these edges lead to series solutions without a subexponential part.

Now fix one of the eligible values for c. For this choice of c and a symbolic parameter s, the coefficient of the dominant term of $L \cdot e^{sx^c}$ will be a polynomial in s. In order to cancel it, we must set s to one of the roots of this polynomial. In order to turn the operator L for $f(x) = e^{sx^c}g(x)$ into an operator $\tilde{L}$ for $g(x)$, recall that the action of operators is compatible with multiplication in the sense that $L \cdot (xf(x)) = (Lx) \cdot f(x)$, where Lx is the product of the operators L and x, whereas $\cdot$ refers to operator application. In this spirit, we would like to say $L \cdot (e^{sx^c}g(x)) = (Le^{sx^c}) \cdot g(x)$, but this does not make sense because e^{sx^c} is not an element of the operator's coefficient domain $C[[x^{-1/v}]]$. However, by the way the shift acts on e^{sx^c}, we know that $e^{-sx^{u/w}}(S^i \cdot e^{sx^{u/w}}) = e^{s(x+i)^{u/w} - sx^{u/w}}$ is an element of $C[[x^{-1/w}]]$, and such series are allowed to appear as coefficients of the operators we consider here. Therefore, while Le^{sx^c} is not a linear difference operator whose coefficients are descending series in x, the operator $\tilde{L} := \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$ is well-defined in this sense. Note however that if the coefficients of L belong to $C[[x^{-1/v}]]$, the coefficients of $\tilde{L}$ belong to $C[[x^{-1/\mathrm{lcm}(v,w)}]]$, where w is the denominator of c.

How is the Newton polygon for $\tilde{L}$ related to the Newton polygon for L? The transition can be divided into two steps. First, when we form $\tilde{L} := \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$ for a parameter s, the selected edge gets prolonged towards the left until it meets the vertical axis. The coefficients of the terms corresponding to points of the prolonged edge are then polynomials in s. In the second step, we instantiate the parameter s to a root of the polynomial associated to the point where the prolonged edge meets the vertical axis. This will have the effect that some part of the selected edge breaks off, meaning that the leftmost part of this edge will get replaced by one or more edges with larger slopes.



The following lemma says that these pictures accurately describe what happens. It implies in addition that the width of the prolonged edge which breaks off in the second step is exactly the multiplicity of the root which is substituted for s.

Lemma 2.45 *(See Lemma 3.44 for the differential case) Let $c = \frac{u}{v} \in \mathbb{Q}$ be such that $0 < c < 1$. Let L be a difference operator with coefficients in $C[[x^{-1/v}]]$, and let $\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$. The coefficients of $\tilde{L}$ are understood as elements of $C[s][[x^{-1/v}]]$. Write*

$$L = \sum_{i=0}^{r} \sum_{j=0}^{\infty} q_{i,j} x^{-j/v} \Delta^i \quad \text{and} \quad \tilde{L} = \sum_{i=0}^{r} \sum_{j=0}^{\infty} \tilde{q}_{i,j} x^{-j/v} \Delta^i.$$

Let $j_0 \in \mathbb{N}$ be minimal such that there exists some i with $j_0 + v(c-1)i \in \mathbb{N}$ and $q_{i,j_0+v(c-1)i} \neq 0$. Let $i_{\min}$ be the smallest and $i_{\max}$ be the largest such i. Finally, let

$$\mu := \sum_{i=i_{\min}}^{i_{\max}} q_{i,j_0+v(c-1)i}\,(cs)^i \in C[s].$$

Then we have:

1. *$\tilde{q}_{i,j} = 0$ for all (i,j) with $j < j_0 + v(c-1)i$,*
2. *$\tilde{q}_{i,j_0+v(c-1)i} = c^{-i} i! \frac{d^i}{ds^i} \mu$ for $i = 0, \ldots, r$, and*
3. *if μ has a nonzero root of multiplicity $i_{\max}$, then $vc \in \mathbb{Z}$.*

Proof According to the general commutation rule for the forward difference Δ, we have $\Delta f(x) = f(x+1)\Delta + (\Delta \cdot f(x))$ for any series $f(x) \in C[[x^{-1/v}]]$. In the expression on the right hand side, the first summand is the action Δ followed by a multiplication by $f(x+1)$, whereas the second summand acts as multiplication by the series $\Delta \cdot f(x)$. More generally, by the binomial theorem, we have the commutation rule $\Delta^i f(x) = \sum_{k=0}^{i} \binom{i}{k}(\Delta^{i-k} \cdot f(x+k))\Delta^k$, in which the summand $(\Delta^{i-k} \cdot f(x+k))\Delta^k$ corresponds to a k-fold application of Δ followed by a multiplication by the series $(\Delta^{i-k} \cdot f(x+k))$. Using this commutation rule, we can calculate

$$\begin{aligned}
\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c} &= \sum_{i=0}^{r}\sum_{j=0}^{\infty} q_{i,j} x^{-j/v} \mathrm{e}^{-sx^c} \Delta^i \mathrm{e}^{sx^c} \\
&= \sum_{i=0}^{r}\sum_{j=0}^{\infty} q_{i,j} x^{-j/v} \sum_{k=0}^{i} \binom{i}{k} \underbrace{\mathrm{e}^{-sx^c} (\Delta^{i-k} \cdot \mathrm{e}^{s(x+k)^c})}_{=(scx^{c-1})^{i-k}+\cdots} \Delta^k \\
&= \sum_{k=0}^{r} \Bigg(\sum_{i=k}^{r} \binom{i}{k} (cs)^{i-k} \underbrace{\sum_{j=0}^{\infty} q_{i,j} \big(x^{-j/v+(c-1)(i-k)} + \cdots \big)}_{=q_{i,j_0+v(c-1)i}\, x^{-j_0/v-(c-1)k}+\cdots} \Bigg) \Delta^k \\
&= \sum_{k=0}^{r} \Bigg(\bigg(\underbrace{\sum_{i=k}^{r} \binom{i}{k} q_{i,j_0+v(c-1)i} (cs)^{i-k}}_{=c^{-k}k!\frac{d^k}{ds^k}\mu} \bigg) x^{-j_0/v-(c-1)k} + \cdots \Bigg) \Delta^k.
\end{aligned}$$

In the last step we used $\binom{i}{k} = \frac{i^{\underline{k}}}{k!}$. After exchanging i and k, we have proved claims 1 and 2.

For the third claim, suppose that $\mu = \tau(s-\sigma)^{i_{\max}}$ for some constants $\tau, \sigma \in C$. Then, by the binomial theorem, the coefficient of s^i in μ is nonzero for every $i = 0, \ldots, r$. This means $q_{i,j_0+v(c-1)i} \neq 0$ for $i = 0, \ldots, r$. Then $j_0 + v(c-1)i \in \mathbb{Z}$ for $i = 0, \ldots, r$, and then $vc \in \mathbb{Z}$, as claimed. ∎

Using this lemma, we can show next that the edge corresponding to terms e^{sx^c} gives rise to as many linearly independent solutions with a subexponential part whose dominant term is e^{sx^c} as the width of the edge indicates. Again, the width refers to the horizontal distance of the leftmost and the rightmost term belonging to the edge. Note that the sum of the widths of all edges of the Newton polygon is exactly the smallest ℓ for which L contains a term $x^0\Delta^\ell$, and this in turn is exactly the multiplicity of $x-1$ in the characteristic polynomial of the recurrence.

Theorem 2.46 *Suppose that C is algebraically closed. Consider a linear recurrence with coefficients in $C[[x^{-1/v}]]$. Let $\ell \in \mathbb{N}$ be the multiplicity of $x-1$ in the characteristic polynomial χ of the recurrence. (It is assumed that $\ell \neq 0$.) Then* *the recurrence has (at least)* ℓ *linearly independent generalized series solutions of the form* $\exp(s_1x^{c_1} + \cdots + s_mx^{c_m})x^{\alpha}a(x)$ *with* $s_1, \dots, s_m \in C$*, rational numbers* $c_1, \dots, c_m$ *with* $0 < c_i < 1$ *for all* i*, some constant* $\alpha \in C$ *and a series* $a(x) \in C[[x^{-1/w}]][\log(x)]$*, for some* $w \in \mathbb{N}$. □

Proof By induction on i, we will show the following: for every operator whose Newton polygon contains an edge whose rightmost vertex lies on the vertical line through $(i, 0)$, there are at least i solutions of the announced type. The choice $i = \ell$ gives the theorem.

For the induction base $i = 0$ there is nothing to show. We will show that the claim is true for i provided that it is true for all smaller natural numbers. Consider an operator L for which the Newton polygon has an edge whose rightmost vertex lies on the vertical line through $(i, 0)$. If the slope of this edge is 1, then we get i linearly independent solutions from Theorem 2.41. If it is not 1, then it can only be smaller than 1. In this case, let c be such that $1 - c$ is the slope of the edge under consideration, and consider the operator $\tilde{L} = \mathrm{e}^{-sx^c}L\mathrm{e}^{sx^c}$ and the polynomial $\mu \in C[s]$ of Lemma 2.45. Note that $\deg\mu = i$.

First consider the case when μ only has roots of multiplicity $< i$. Let $\sigma_1, \dots, \sigma_m \in C$ be the nonzero roots of μ and let $e_1, \dots, e_m$ be their multiplicities. Let $i_{\min}$ be the multiplicity of 0 in μ. We then have $i_{\min} + e_1 + \cdots + e_m = i$. By the induction hypothesis, we obtain $i_{\min}$ many linearly independent solutions from the edges to the left of the current edge. Furthermore, setting s to one of the roots σ_j in $\tilde{L}$ leads to an operator in which a part of length e_j of the prolonged edge is replaced by edges of steeper slope. Again by the induction hypothesis, we obtain e_j many linearly independent solutions of $\tilde{L}$ corresponding to these new edges. Multiplying them with $\mathrm{e}^{\sigma_j x^c}$ turns them into solutions of L. Altogether, we obtain $i = i_{\min} + e_1 + \cdots + e_m$ solutions. The set of all these solutions is linearly independent because the various linearly independent sets of series obtained through the induction hypothesis are multiplied by distinct dominant terms $\mathrm{e}^{\sigma x^c}$.

It remains to consider the case when μ has only a single root σ of multiplicity i. In this case, we have $vc \in \mathbb{Z}$ by part 3 of Lemma 2.45. Therefore, in this case the coefficients of $\tilde{L}$ again belong to $C[[x^{-1/v}]]$. Setting s to be the unique root of μ will lead to a Newton polygon in which the entire edge of slope $1 - c$ is replaced by one or more steeper edges. Let $\tilde{c}$ be such that $1 - \tilde{c}$ is the slope of the rightmost new edge, let $\tilde{\tilde{L}} = \mathrm{e}^{-sx^{\tilde{c}}}\tilde{L}\mathrm{e}^{sx^{\tilde{c}}}$, and let $\tilde{\mu}$ be the corresponding polynomial as in Lemma 2.45. If $\tilde{\mu}$ has only roots of multiplicity $< i$, we can argue as before and obtain i linearly independent solutions of $\tilde{L}$. Multiplication by $\mathrm{e}^{\sigma x^c}$ turns them into solutions of L. If $\tilde{\mu}$ again has only a single root of multiplicity i, then $v\tilde{c} \in \mathbb{Z}$ by part 3 of Lemma 2.45, and thus the coefficients of $\tilde{\tilde{L}}$ still belong to $C[[x^{-1/v}]]$. Because of $\tilde{c} \le c - \frac{1}{v}$, after at most v repetitions of the argument, we either encounter an edge of width i and slope 1 (and then we can use Theorem 2.41) or we encounter a Newton polygon to which the argument of the previous paragraph applies. ■

Example 2.47 Consider the operator $L = x^{-1}\Delta^3 + \Delta^5$ from the previous example. The indicial polynomial is cubic and signals the exact solutions $1, x, x^2$. There are two more solutions corresponding to the edge of slope 1/2. For a symbolic parameter s, the operator $\tilde{L} = \mathrm{e}^{-sx^{1/2}} L \mathrm{e}^{sx^{1/2}}$ has the form

$$\tilde{L} = \Big(\frac{4s^3 - s^5}{32} x^{-5/2} + \cdots\Big) + \Big(\frac{12s^2 - 5s^4}{16} x^{-2} + \cdots\Big)\Delta + \Big(\frac{6s - 5s^3}{4} x^{-3/2} + \cdots\Big)\Delta^2$$
$$+ \Big(\frac{2 - 5s^2}{2} x^{-1} + \cdots\Big)\Delta^3 + \Big(-\frac{5s}{2} x^{-1/2} + \cdots\Big)\Delta^4 + \Big(-1 + \cdots\Big)\Delta^5.$$

The polynomial $\mu = (4s^3 - s^5)/32$ has two nonzero roots, 2 and -2, and they are both simple. Setting $s = 2$ leads to the operator

$$\begin{aligned}\tilde{L} &= (\tfrac{5}{2}x^{-3} + \tfrac{5}{3}x^{-7/2} + \cdots) + (-2x^{-2} + \tfrac{9}{2}x^{-5/2} + \tfrac{181}{6}x^{-3} + \cdots)\Delta \\ &+ (-7x^{-3/2} - \tfrac{25}{2}x^{-2} + \tfrac{163}{4}x^{-5/2} + \cdots)\Delta^2 \\ &+ (-9x^{-1} - 32x^{-3/2} - \tfrac{49}{3}x^{-2} + \cdots)\Delta^3 \\ &+ (-5x^{-1/2} - \tfrac{45}{2}x^{-1} - \tfrac{475}{12}x^{-3/2} + \cdots)\Delta^4 \\ &+ (-1 - 5x^{-1/2} - \tfrac{25}{2}x^{-1} + \cdots)\Delta^5.\end{aligned}$$

The solution space of this operator in $C[[x^{-1/2}]]$ is generated by

$$x^{5/4}\Big(1 - \tfrac{245}{48}x^{-1/2} + \tfrac{39937}{4608}x^{-1} - \tfrac{18041953}{3317760}x^{-3/2} + \cdots\Big).$$

Multiplying this series by $\mathrm{e}^{2x^{1/2}}$ gives a solution of L. The solution corresponding to the choice $s = -2$ is essentially the same, only the signs of the coefficients of $x^{-j/2}$ with odd j in the series expansion are flipped. □

The rest of the story is much simpler. The solutions discussed so far all originate from the factor $x - 1$ of the characteristic polynomial. We find as many solutions as the multiplicity of this factor. All of these solutions have a trivial exponential part 1^x, and it turns out that the other factors $x - \phi$ of the characteristic polynomial give rise to solutions with an exponential part ϕ^x. To see this, suppose we have $f(x) = \phi^x g(x)$ for some nonzero constant $\phi \in C$ and some $f(x)$ and $g(x)$. Then we have

$$\begin{aligned} & p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0 \\ \iff\quad & p_0(x)g(x) + p_1(x)\phi g(x+1) + \cdots + p_r(x)\phi^r g(x+r) = 0\end{aligned}$$

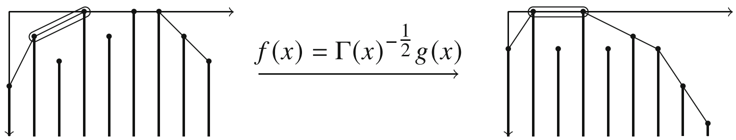
for any $p_0, \ldots, p_r \in C[[x^{-1/v}]]$. Thus any recurrence for $f(x)$ can be translated into a recurrence for $g(x)$, and if $\chi(x) \in C[x]$ is the characteristic polynomial of the recurrence for $f(x)$ then $\chi(\phi x) \in C[x]$ is the characteristic polynomial of the recurrence for $g(x)$. This follows directly from Definition 2.37. Because of $(\phi - x)^\ell \mid \chi \iff (1 - x)^\ell \mid \chi(\phi x)$, the solutions of the recurrence for $f(x)$

with exponential part ϕ^x are precisely the solutions of the recurrence for $g(x)$ with exponential part 1^x, and we already know how to determine these. In summary, we can thus find altogether $\deg(\chi) - \nu(\chi)$ linearly independent solutions of the recurrence for $f(x)$, where $\nu(\chi)$ denotes the multiplicity of x in χ.

If $\nu(\chi) > 0$ or $\deg(\chi) < r$, then we can obtain further solutions by applying another type of substitution. Suppose we have $f(x) = \Gamma(x)^{u/w} g(x)$ for some $u/w \in \mathbb{Q}$ and some series $f(x)$ and $g(x)$. Then, because of $\Gamma(x+1) = x\Gamma(x)$, we have

$$\begin{aligned} & p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0 \\ \iff \quad & p_0(x)g(x) + p_1(x)x^{u/w}g(x+1) + \cdots + p_r(x)(x^{\overline{r}})^{u/w}g(x+r) = 0 \end{aligned}$$

for all $p_0, \ldots, p_r \in C[[x^{-1/v}]]$. Note that the coefficients of the second recurrence belong to $C[[x^{-1/(vw)}]]$. Similar as in the construction of subexponential parts, the effect of the substitution admits a simple geometric interpretation. For each coefficient p_i of the recurrence for $f(x)$, let e_i be maximal such that the coefficient of x^{e_i} in p_i is nonzero. (For $p_i = 0$ take $e_i = -\infty$.) Draw a vertical halfline in $\mathbb{R}^2$ from (i, e_i) downwards and consider the convex hull of these halflines. The characteristic polynomial corresponds to horizontal segment of this polygon (if there is no such segment, regard the highest point of the polygon as a segment of length 0). A substitution $f(x) = \Gamma(x)^{u/w} g(x)$ turns the recurrence for $f(x)$ into a recurrence for $g(x)$ which is such that the segment with slope $-u/w$ in the recurrence for $f(x)$ translates into a horizontal segment in the recurrence for $g(x)$.



For every segment in the convex hull there is a substitution which turns the segment into a horizontal segment without changing its width. If χ is the characteristic polynomial of the new recurrence, then $\deg(\chi) - \nu(\chi)$ is exactly the width of this segment, and by the preceding discussion we know how to find $\deg(\chi) - \nu(\chi)$ linearly independent solutions for it. The number of solutions we obtain altogether for the original recurrence is thus the sum of the widths of all segments. If p_0 is not zero (which we may assume without loss of generality), this sum is equal to the order r of the recurrence. Putting all the constructions discussed in this section together leads to the following theorem.

Theorem 2.48 *(See Theorem 3.45 for the differential case) Suppose C is algebraically closed. Let $p_0, \ldots, p_r \in C[[x^{-1/v}]]$, $p_0, p_r \neq 0$. Then there are r linearly independent generalized series*

$$f(x) = \Gamma(x)^{u/w}\phi^x \exp(s_1 x^{1/w} + \cdots + s_{w-1}x^{(w-1)/w})x^\alpha a(x^{-1/w}, \log(x))$$

for some $w \in \mathbb{N}$, $u \in \mathbb{Z}$, $\phi, \alpha, s_1, \ldots, s_{w-1} \in C$, *and* $a \in C[[x]][y]$, *such that*

$$p_0(x)f(x) + p_1(x)f(x+1) + \cdots + p_r(x)f(x+r) = 0.$$

□

According to Exercises 9 and 10, the set of all C-linear combinations of generalized series without exponential part forms an integral difference ring R with constant field C. Exercise 9 also implies that R contains no elements u with $\sigma(u)/u \in C \setminus \{1\}$. If we take as K the fraction field of R, then the r generalized series announced in Theorem 2.48 can be viewed as elements of a difference ring $K[\phi_1^x, \ldots, \phi_r^x]$ that meets the requirements of Theorem 2.29. This implies that additional generalized series solutions cannot exist. We have found them all. In particular, we can drop the "at least" from the statements of Theorem 2.41 (part 1) and Theorem 2.46.

Exercises

1**.** Let $p_0, \ldots, p_r, f \in C[[x^{-1/v}]]$, and write $p_i = \sum_{j=0}^{\infty} p_{i,j} x^{-j/v}$ ($i = 0, \ldots, r$) and $f = \sum_{n=0}^{\infty} c_n x^{-n/v}$. Show that

$$\sum_{i=0}^{r} p_i(x) f(x+i) = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} c_{n-j} \sum_{k=0}^{\lfloor j/v \rfloor} \binom{-(n-j)/v}{k} \sum_{i=0}^{r} p_{i,j-vk} i^k \right) x^{-n/v}.$$

2.** For the first recurrence in Example 2.36, determine the multiplicative constant in the asymptotic growth for the sequence solution with initial values $f(0) = 0$, $f(1) = 1$. Which choices of initial values exhibit an asymptotic expansion that corresponds to the second generalized series solution?

3. Determine the generalized series solutions of the recurrences in Examples 2.3 and 2.4. Explain why the error propagation is stronger for the recurrence of Example 2.4.

4. Let $p_0, \ldots, p_r \in C[x]$ be such that $\deg p_i \leq \deg p_r$ for all i. Show that the roots of the characteristic polynomial of the recurrence $p_0(n)f(n) + \cdots + p_r(n)f(n+r) = 0$ are precisely the eigenvalues of the limiting matrix $\lim_{n\to\infty} P(n)$, where $P(x) \in C(x)^{r\times r}$ is the companion matrix of the recurrence.

5. Find the generalized series solutions of the following recurrences:

a. $(x+2)f(x+2) - (6x+9)f(x+1) + (5x+5)f(x) = 0$;

b. $(x+2)^2 f(x+2) - (7x^2+21x+16)f(x+1) - 8(x+1)^2 f(x) = 0$;

c. $2(x^2+3x+2)f(x+2) - (3x^2+10x+7)f(x+1) + (x^2+4x+4)f(x) = 0$.

Hint: There are no subexponential parts and no logarithmic terms in these examples.

6. Find the generalized series solutions of the following recurrences:

a. $(3x+5)f(x)+(6x+13)f(x+1)+(3x+8)f(x+2)=0$;

b. $2(2x+3)f(x)-2(4x+9)f(x+1)+(4x+3)f(x+2)=0$;

c. $(2x-8x^{1/2}+3)f(x)-(4x-12x^{1/2}-1)f(x+1)+2(x-2x^{1/2}-1)$ $f(x+2)=0$.

Hint: There are subexponential parts and/or logarithmic terms in these examples.

7. Construct a linear recurrence with polynomial coefficients which has a generalized series solution starting like

$$9^x x^{-\frac{1}{2}}\Big(1-\tfrac{3}{32}x^{-1}+\tfrac{49}{2048}x^{-2}+\tfrac{1335}{65536}x^{-3}+\tfrac{178059}{8388608}x^{-4}$$
$$+\tfrac{10728963}{268435456}x^{-5}+\tfrac{1680819701}{17179869184}x^{-6}+\cdots\Big).$$

Hint: There is one of order two with polynomial coefficients of degree one.

8****.** Show that $\log(x)$ does not satisfy a linear recurrence with polynomial coefficients.

Hint: You may use without proof that for any pairwise distinct $\phi_1,\dots,\phi_r\in C$ the sequences $(\phi_i^n)_{n=0}^{\infty}$ are linearly independent over $C(n)$.

9****.** **a.** Show that if $f\in C[[[x^{-1/v}]]]$ and $c\in C\setminus\{0\}$ are such that $f(x+1)-cf(x)=0$, then $c=1$ and $f\in C$.

b. Show that if f is an arbitrary generalized series and $c\in C\setminus\{0\}$ is such that $f(x+1)-cf(x)=0$, then $c=1$ and $f\in C$.

c. Show that if f is a C-linear combination of generalized series and $c\in C\setminus\{0\}$ is such that $f(x+1)-cf(x)=0$, then $c=1$ and $f\in C$.

10*****.** (Silviu Radu)

a. Let $\alpha_1,\dots,\alpha_m\in C$ be such that $1,\alpha_1,\dots,\alpha_m$ are linearly independent over $\mathbb{Q}$. Let $k_1,\dots,k_n$ be pairwise distinct positive integers, and for each $i\in\{1,\dots,n\}$, let $\beta_{i,1},\dots,\beta_{i,m}\in C$ be linearly independent over $\mathbb{Q}$. Show that the terms $\Gamma(x)$, $\exp(\beta_{i,j}x^{k_i})$ ($i=1,\dots,n$; $j=1,\dots,m$), and x^{α_ℓ} ($\ell=1,\dots,m$) are algebraically independent over $C[[x^{-1}]][\log(x)]$.

b. Show that the set of all linear combinations of generalized series without exponential part (i.e., with $\phi=1$) forms an integral domain.

11***.** Let S denote the shift operator mapping x to $x+1$ and $\frac{d}{dq}$ the derivation with respect to q. Show that $S\frac{d}{dq}\cdot f(x,q)=\frac{d}{dq}S\cdot f(x,q)$ for all $f(x,q)\in x^qC(q)[[x^{-1/v}]][\log(x)]$.

12***.** Consider a linear recurrence with coefficients in $C[[x^{-1}]]$. Show that if $f(x)$ is a solution in $C[[x^{-1}]][\log(x)]$ of degree d with respect to $\log(x)$, then $[\log(x)^d]f(x)\in C[[x^{-1}]]$ is also a solution of the recurrence.

13******.** Consider a recurrence operator $L=\sum_{i=0}^{r}\sum_{j=0}^{\infty}p_{i,j}x^{-j}S^i$. (For simplicity we restrict to $v=1$.) According to Definition 2.37, the indicial polynomial of

L is $\eta = \sum_{k=0}^{j} \binom{-x}{k} \sum_{i=0}^{r} p_{i,j-k} i^k$, where j is minimal such that η is nonzero. Show that the discussion before Example 2.43 leads to the alternative form $\tilde{\eta} = \sum_{i=0}^{j} \binom{-x}{k} \sum_{i=0}^{r} p_{i,j-k} i^{\underline{k}}$, where j is minimal such that $\tilde{\eta}$ is nonzero. Why is $\tilde{\eta} = \eta$?

14*. Characterize all generalized series which can arise as solutions of a recurrence $p_0(x)f(x) + p_1(x)f(x+1) = 0$ with $p_0, p_1 \in C[[x^{-1}]] \setminus \{0\}$.

15. Find the first few terms of a generalized series solution f of the inhomogeneous recurrence equation $f(x+1) - f(x) = \Gamma(x)\phi^x x^\alpha$.

16. Show that the recurrence

$$2(2x+1)^2 f(x) - (12x^2 + 8x - 3) f(x+1) + 2(x+1)(2x-1) f(x+2) = 0$$

has no solution in $C(x)$. *Hint:* Any rational solution gives rise to a generalized series solution of a special kind.

17*. Let $p_0, \dots, p_r \in C[x]$ and let $q_0, \dots, q_s \in C[x]$ be such that $q_0(x)a(x) + \cdots + q_s(x)a^{(s)}(x) = 0$ is the differential equation obtained by the construction of Theorem 2.33 from the recurrence $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$. Let $\chi \in C[x]$ be the characteristic polynomial of the recurrence. Show that $x^{\deg \chi} \chi(1/x)$ divides q_s.

18*. Let p be a positive integer and consider a linear recurrence with coefficients in $C[[x^{-1}]]$ (i.e., $v = 1$). Suppose that the recurrence has a solution whose subexponential part is $\mathrm{e}^{x^{1/p}}$. Show that the order of the recurrence is at least p. Show also that when ω is a pth root of unity in C, then the recurrence also has a generalized series solution whose subexponential part is $\mathrm{e}^{\omega x^{1/p}}$.

19. Why is it not necessary to also include terms e^{x^c} with **a.** $c \le 0$, or **b.** $c > 1$ in the subexponential part?

20.** Let $f_1(x), \dots, f_r(x)$ be C-linearly independent generalized series without logarithmic terms. Show that there is a linear recurrence with coefficients in $C[[x^{-1/v}]]$, for a suitable $v \in \mathbb{N}$, which has $f_1(x), \dots, f_r(x)$ among its solutions. (It is not necessary to exclude series with logarithmic terms, but the argument is a bit simpler in this situation.)

References

The construction of a procedure for finding generalized series solutions of linear recurrences was initiated when Poincare introduced the notion of asymptotic expansions [359], and it was not completed until the 1930s, when Adams [28], Birkhoff [66, 67], and Trjitzinsky [68] understood how to handle equations whose solutions have subexponential parts in full generality. The corresponding procedure for the differential case (cf. Sect. 3.4) was already known and served as a guideline of the development.

Unlike our presentation, in which generalized series are viewed as algebraic objects, these early authors interpreted them as analytic objects and wondered about how the series solutions are related to the asymptotic expansions of function solutions defined on $\mathbb{R}$ or $\mathbb{C}$ when x is sent to infinity. With respect to this relationship, the paper of Birkhoff and Trjitzinsky contains assertions whose proofs are flawed, see Sect. 9.2 of Odlyzko's survey [342] for a discussion and the paper of Braaksma, Faber, and Immink [106] for some more recent results.

Wimp and Zeilberger [459] promoted the use of generalized series solutions of linear recurrence equations and point out that for many examples, generalized series solutions can be easily identified, at least experimentally, as asymptotic expansions of sequence solutions as we showed in Example 2.36. Note however that the multiplicative constant of the asymptotic expansion can usually only be computed numerically. If a D-finite sequence can be expressed as the diagonal of a multivariate rational power series (cf. Definition 5.32), alternative methods for determining its asymptotics are available that also deliver exact expressions for the multiplicative constant [321, 330, 353].

2.5 Polynomial and Rational Solutions

So far we discussed the computation of sequence or series solutions to a given linear recurrence. These are infinite objects which we cannot hope to write down in their entirety. The algorithms that have been presented so far determined only an arbitrarily large finite portion of them.

We now turn to the search for solutions of linear recurrences which can be expressed in a closed form. There is no precise definition of what a closed form is, but informally, the notion refers to solutions which can be written down by some type of finite expression.

Given a linear recurrence with polynomial coefficients, there is a relatively straightforward way to find all polynomial solutions of a prescribed maximal degree $n \in \mathbb{N}$. It suffices to make an ansatz $f = \sum_{k=0}^{n} a_k x^k$ with undetermined coefficients, plug the ansatz into the equation, equate like powers of x to zero, and solve the resulting linear system for the unknown coefficients $a_0, \ldots, a_n$.

Example 2.49 Consider the recurrence

$$(10 + 3x)(13 + 3x) f(x) + 6(17 + 6x) f(x + 1) - (4 + 3x)(7 + 3x) f(x + 2) = 0.$$

We want to know all solutions in $C[x]$ of degree at most four. Consider an ansatz $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$. Substituting $f(x)$ into the recurrence leads to

$$\begin{aligned}&(18a_3 - 132a_4)x^4 + (36a_2 + 6a_3 - 680a_4)x^3\\&\quad + (54a_1 + 108a_2 - 222a_3 - 1116a_4)x^2\\&\quad + (72a_0 + 174a_1 - 4a_2 - 258a_3 - 980a_4)x\\&\quad + (204a_0 + 46a_1 - 10a_2 - 122a_3 - 346a_4) = 0.\end{aligned}$$

Forcing the coefficients of $x^k (k = 0, \ldots, 4)$ to zero leads to the linear system

$$\begin{pmatrix} 0 & 0 & 0 & 18 & -132 \\ 0 & 0 & 36 & 6 & -680 \\ 0 & 54 & 108 & -222 & -1116 \\ 72 & 174 & -4 & -258 & -980 \\ 204 & 46 & -10 & -122 & -346 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

which has a solution space of dimension one spanned by (280, 1254, 1431, 594, 81). It follows that all polynomial solutions of degree at most four are constant multiples of $280 + 1254x + 1431x^2 + 594x^3 + 81x^4$. □

It is clear that the polynomial solutions of degree up to n form a vector space over C, and that the method described above leads to a basis of this vector space. The dimension of the space can be at most $n + 1$. Also when there is no limit on the degree, the dimension of the solution space in $C[x]$ can only be finite. This follows from Theorem 2.26. But then for every given recurrence there must be some $n \in \mathbb{N}$ such that all solutions in $C[x]$ of the recurrence have degree at most n. Such a number n is called a *degree bound.*

In order to find a degree bound, it suffices to note that every polynomial solution is in particular also a generalized series solution of the recurrence. As we have seen in the previous section, the largest exponents arising in a generalized series solution are roots of the indicial polynomial. We can therefore take the largest nonnegative integer root of the indicial polynomial as a degree bound. If the indicial polynomial does not have any nonnegative integer roots, it can be concluded that no polynomial solutions exist.

Once a degree bound is known, we can compute a basis of the solution space in $C[x]$ using linear algebra as in Example 2.49. This is the classical algorithm for finding polynomial solutions. It requires us to solve a linear system over C with $n + 1$ variables and up to $n + d + 1$ equations. Unfortunately, n can be very large. For example, the recurrence $(x + 1000)f(x) - xf(x + 1) = 0$ has the polynomial solution $f(x) = x(x + 1)\cdots(x + 999)$ of degree 1000. We are therefore interested in an algorithm whose complexity is small with respect to n, while the dependence of the complexity on the order r and the degree d is of secondary importance.

The complexity of the classical algorithm is cubic in n (or $\mathrm{O}(n^\omega)$ if fast linear algebra is used). We can do better. One idea is to compute the first few terms of a basis of sequence solutions using the algorithms of Sects. 2.1 and 2.2 and then compute interpolating polynomials for these sequences. If some sequence solution happens to consist of the evaluations of a polynomial solution at the integers, we will notice that from some point on the interpolation polynomial will not change any more if we take into account more terms. On the other hand, in the more likely event that a sequence solution does not correspond to a polynomial solution, the degree of the interpolation polynomial will keep growing as we take into account more interpolation points.

In general, the space of polynomial solutions only corresponds to a subspace of the space of sequence solutions, and we need to separate the sequences in this subspace from the other sequence solutions. This can be done using the following lemma.

Lemma 2.50 *Let $p_0, \ldots, p_r \in C[x]$ and $\deg(p_i) \leq d$ for all i. Let $f \in C[x]$ with $\deg(f) \leq n$ and $g \in C[x]$ with $\deg(g) \leq n + d$. If $\sum_{i=0}^{r} p_i(k) f(k+i) = g(k)$ for $k = 0, \ldots, n+d$, then $\sum_{i=0}^{r} p_i(x) f(x+i) = g(x)$.*

Proof Since $\deg(f) \leq n$ and $\deg(g) \leq n + d$ and $\deg(p_i) \leq d$ for all i, the polynomial

$$\sum_{i=0}^{r} p_i(x) f(x+i) - g(x)$$

has degree at most $n + d$. By assumption, it has at least $n + d + 1$ roots. Therefore it must be the zero polynomial. ■

Algorithm 2.51 *(See Algorithm 3.51 for the differential case)*
Input: $p_0, \ldots, p_r \in C[x]$ *with* $p_r \neq 0$.
Output: *A basis of the space of all* $f \in C[x]$ *such that* $\sum_{i=0}^{r} p_i(x) f(x+i) = 0$.

1 *Choose $\epsilon \in C$ such that $p_r(x+\epsilon)$ has no integer roots.*
2 *Replace p_i by $p_i(x+\epsilon)$ for $i = 0, \ldots, r$.*
3 *Compute the indicial polynomial η (cf. Definition 2.37).*
4 *If η has no roots in $\mathbb{N}$, return $\emptyset$ and stop.*
5 *Let n be the largest integer root of η.*
6 *Using Algorithm 2.1, compute the first $n + d + 1$ terms of a basis of sequence solutions.*
7 *Compute the interpolating polynomials $f_1, \ldots, f_r$ for these sequences.*
8 *Make an ansatz $f = \alpha_1 f_1 + \cdots + \alpha_r f_r$ with undetermined coefficients α_i and equate the coefficients of x^k for $k = n+1, \ldots, n+d$ to zero.*
9 *Solve the resulting linear system, and for each basis element $(\alpha_1, \ldots, \alpha_r)$ of its solution space, return $\alpha_1 f_1(x-\epsilon) + \cdots + \alpha_r f_r(x-\epsilon)$.*

Theorem 2.52 *Algorithm 2.51 is correct and apart from the cost of determining the integer roots of η, it needs no more than $\mathrm{O}(r^2 d(n+d) + r\mathrm{M}(n+d)\log(n+d))$ operations in C, where n is the largest integer root of η.* □

Proof For the complexity, the first term corresponds to the cost of line 6. Note that because of the change of variables in line 1, the space of sequence solutions has exactly dimension r. The second term in the estimate corresponds to the cost of line 7. Solving the linear system in line 9 costs $\mathrm{O}(rd\min(r,d))$ operations; this term is dominated by $r^2d(n+d)$. Note that this is a system with r variables and d equations.

For the correctness, observe first that for all $f \in C[x]$ and all $\epsilon \in C$ we have $\sum_{i=0}^{r} p_i(x)f(x+i) = 0$ if and only if $\sum_{i=0}^{r} p_i(x+\epsilon)f(x+\epsilon+i) = 0$. This justifies the change of variables in lines 1 and 9. Now let V be the solution space of the recurrence in $C[x]$ and let $W \subseteq C[x]$ be the space generated by the polynomials returned by the algorithm. We show that $V = W$.

"$\supseteq$": For every $f \in W$ we have $\deg(f) \leq n$ by the choice of $\alpha_1, \dots, \alpha_r$ and $\sum_{i=0}^{r} p_i(k)f(k+i) = 0$ for $k = 0, \dots, n+d$ by the choice of $f_1, \dots, f_r$. Lemma 2.50 implies that $f \in V$.

"$\subseteq$": Let $f \in V$. By the choice of n we have $\deg(f) \leq n$. The sequence $(f(k))_{k=0}^{\infty}$ is a solution of the recurrence, and therefore a certain linear combination of the basis elements computed in line 6. Therefore, f is a certain linear combination of the polynomials $f_1, \dots, f_r$ obtained in line 7, say $f = \beta_1 f_1 + \dots + \beta_r f_r$ with $\beta_1, \dots, \beta_r \in C$. As f is a solution of the recurrence, we have $\sum_{i=0}^{r} p_i(k)f(k+i) = 0$ for all $k \in \mathbb{N}$, in particular for $k = n+1, \dots, n+d$. Therefore, $(\beta_1, \dots, \beta_r)$ belongs to the solution space of the linear system solved in line 9. It follows that $f \in W$. ■

Algorithm 2.51 outperforms the classical algorithm even when no fast arithmetic is available. In this case, the cost of interpolation is $\mathrm{O}(n^2)$, and this is also the cost of the whole algorithm if we assume $r, d = \mathrm{O}(1)$. It is possible to reduce the complexity further. Observe that every polynomial $f \in C[x]$ of degree n can be written uniquely in the form $f(x) = \sum_{k=0}^{n} a_k \binom{x}{k}$ for some $a_k \in C$. In other words, the polynomials $\binom{x}{0}, \binom{x}{1}, \binom{x}{2}, \dots$ form a basis of $C[x]$. It is called the *binomial basis*. Since the binomial coefficient $\binom{n}{k}$ is zero for $n = 0, \dots, k-1$ and one for $n = k$, the basis makes the execution of an interpolation step particularly easy. In fact, the coefficients a_n are given by $a_n = \sum_{k=0}^{n} (-1)^{k+n} f(k)\binom{n}{k}$. As we see, each coefficient a_n depends only on finitely many sequence terms. We therefore need not restrict ourselves to polynomials but may also consider infinite series $\sum_{k=0}^{\infty} a_k \binom{x}{k}$, the so-called binomial series. There is a one-to-one correspondence between the binomial series solutions of a recurrence and its sequence solutions. The key observation is that whenever $(u_n)_{n=0}^{\infty}$ is a D-finite sequence, then so is the sequence $(a_n)_{n=0}^{\infty}$ defined by $a_n = \sum_{k=0}^{n} (-1)^{k+n} u_k \binom{n}{k}$ for all $n \in \mathbb{N}$.

Proposition 2.53 *Let* $p_0, \dots, p_r \in C[x]$ *with* $p_r \neq 0$ *be such that* $\deg(p_i) \leq d$ *for all* i. *Let* $f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ *be such that* $p_0(x)f(x) + \dots + p_r(x)f(x+r) = 0$ *for all* $x \in \mathbb{N}$. *Then* $(a_n)_{n=0}^{\infty}$ *satisfies a recurrence of order* $r+d$ *and degree* d *whose leading coefficient is (up to shift) equal to* p_r. □

Proof Write the recurrence for $f(x)$ as the operator $L = \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}x^j S_x^i$, where S_x denotes the shift operator acting like $S_x \cdot f(x) = f(x+1)$. Since shift and multiplication by x act on a basis element $\binom{x}{n}$ via

$$\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1} \quad \text{and} \quad x\binom{x}{n} = n\binom{x}{n} + (n+1)\binom{x}{n+1},$$

the annihilating operator L for $f(x)$ translates into an annihilating operator

$$M = \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}(n(1+S_n^{-1}))^j(1+S_n)^i$$

for the sequence $(a_n)_{n=0}^{\infty}$. Then also $S_n^d M$ is an annihilating operator for $(a_n)_{n=0}^{\infty}$, and this latter operator has order at most $r+d$ and degree at most d.

The coefficient of S_n^r in M above is $\sum_{j=0}^{d} p_{r,j}n^j$. Hence the coefficient of S_n^{r+d} in $S_n^d M$ is $\sum_{j=0}^{d} p_{r,j}(n+d)^j$, which is indeed a shifted version of the leading coefficient of L. ■

Using Proposition 2.53, we can evaluate the coefficients $a_0, a_1, \dots, a_n$ for the interpolating polynomials $f_1, \dots, f_r$ in Algorithm 2.51 using no more than $\mathrm{O}(n)$ operations (again assuming $r, d = \mathrm{O}(1)$ for simplicity). Of course, the comparison with Algorithm 2.51 is only fair if we return the polynomials with respect to the standard basis $1, x, x^2, \dots$, and the basis conversion from a binomial basis to the standard basis may cost up to $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations. Note however that while in Algorithm 2.51 we always perform r calls to the interpolation algorithm, the number of basis conversions is determined by the number of polynomial solutions. Although there can be up to r linearly independent polynomial solutions in general, generically there will be much fewer. Further improvement is possible by using the recurrence for a_n backwards. In this version, we start with $a_n = 0$ for all sufficiently large n and work downwards. Only when n is a root of the trailing coefficient of the recurrence, a solution can start to be nonzero, and then the recurrence determines its subsequent terms. We continue the computation down to $a_{-r-d}, \dots, a_{-1}$ and find all linear combinations for which these terms are zero. The advantage of this approach is that the number of solutions whose terms we need to compute is bounded by the number of nonnegative integer roots of the trailing coefficient of the recurrence for a_n, which may be smaller than r.

The D-finiteness of the sequence $(a_n)_{n=0}^{\infty}$ also allows us to test quickly whether polynomial solutions exist at all. Using Algorithm 2.8, we can compute the terms $a_{n+1}, \dots, a_{n+d+r}$ for the r elements of a basis of sequence solutions with only $\mathrm{O}(\sqrt{n})$ operations in C (assuming $d, r = \mathrm{O}(1)$). As we have seen above, a polynomial solution exists if and only if the vectors $(a_{n+1}, \dots, a_{n+d+r}) \in C^{d+r}$ are linearly dependent. The time for checking this is independent of n and therefore negligible when n is sufficiently large.

Although it is easy to construct recurrence equations that have polynomial solutions which are much larger than the equations, such situations are not common. Recurrence equations naturally arising from applications tend to have indicial polynomials with reasonably sized integer roots. Many of these equations have indicial polynomials with no integer roots at all, so that the absence of polynomial solutions can be concluded without any further calculation. Others do have integer roots, but their values do not exceed the degree d, so that the assumption that n is large compared to r and d is not adequate. In view of these circumstances, it is not surprising that many implementations nowadays still rely on the "naive" algorithm based on linear algebra.

All of the algorithms discussed so far can be easily extended to inhomogeneous equations with polynomial right hand sides. The solution set of a recurrence

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x)$$

with given $p_0, \dots, p_r, g \in C[x]$ and unknown $f \in C[x]$ is an affine linear subspace of $C[x]$. Clearly, the difference between any two solutions is a solution of the corresponding homogeneous equation (the equation where the right hand side g is replaced by 0). As it is more convenient to reason about vector spaces, we will consider a homogenized version of the equation in which the right hand side g is replaced by cg for an unknown constant c. The solution set of such a recurrence is then a linear subspace V of $C[x] \times C$ consisting of all pairs (f, c) for which the equation is satisfied. The pairs in V for which the second component is equal to 1 forms the solution set of the inhomogeneous equation.

Homogenization also allows us to consider several right hand sides simultaneously. For given $p_0, \dots, p_r \in C[x]$ and $g_1, \dots, g_m \in C[x]$, we can ask for (a basis of) the vector space consisting of all tuples $(f, c_1, \dots, c_m) \in C[x] \times C^m$ such that

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = c_1g_1(x) + \cdots + c_mg_m(x).$$

Such an equation is called a *parameterized linear recurrence.*

Example 2.54

1. The solution space in $C[x] \times C^2$ of the parameterized recurrence

$$(x+1)^2f(x+2) - 2(x+2)^2f(x+1) + (x+3)^2f(x) = c_1(3x+1) + c_2(2x+1)$$

is generated by $(1, -4, 6)$ and $(x, 10, -16)$.

2. The solution space in $C[x] \times C^2$ of the parameterized recurrence

$$(x+1)f(x+2) - (x+2)f(x+1) + (x+3)f(x) = c_1(3x+1)^2 + c_2(2x+1)^2$$

is generated by $(19x + 13, -17, 43)$.

□

Lemma 2.55 *Let $p_0, \ldots, p_r \in C[x]$ be such that $\deg_x(p_i) \leq d$ for $i = 0, \ldots, r$. Let η be the indicial polynomial for $p_0, \ldots, p_r$. Let $f \in C[x]$ and let $n = \deg_x(f)$. If*

$$\deg_x(p_0(x)f(x) + \cdots + p_r(x)f(x+r)) < n + d - \deg(\eta),$$

then $\eta(n) = 0$.

Proof Write the operator $L = \sum_{i=0}^r p_i(x)S^i$ in the form $L = \sum_{i=0}^r q_i(x)\Delta^i$ with $q_i(x) = \sum_{k=i}^r \binom{k}{i} p_k(x)$ for $i = 0, \ldots, r$, and write $q_i(x) = \sum_{j=0}^d q_{i,j}x^j$ for constants $q_{i,j} \in C$. As already argued in Sect. 2.4 (see also Exercise 13 of that section), we have

$$L \cdot (x^n + \cdots) = \sum_{i=0}^r \sum_{j=0}^d q_{i,j}x^j(n^{\underline{i}}x^{n-i} + \cdots) = \eta(n)x^{n+d-\deg(\eta)} + \cdots$$

for every $n \in \mathbb{N}$. The claim follows. ∎

Algorithm 2.56 *(See Algorithm 3.56 for the differential case)*
Input: $p_0, \ldots, p_r \in C[x]$ *and* $g_1, \ldots, g_m \in C[x]$.
Output: *A basis of the* C*-vector space of all* $(f, c_1, \ldots, c_m) \in C[x] \times C^m$ *such that*

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = c_1g_1(x) + \cdots + c_mg_m(x).$$

1. *Compute the indicial polynomial η (cf. Definition 2.37) for $p_0, \ldots, p_r$, and let $\xi_1, \ldots, \xi_k$ be its roots in $\mathbb{N}$ (if there are any).*
2. *Set $d = \max_{i=0}^r \deg_x(p_i)$ and*
   $n = \max\{\xi_1, \ldots, \xi_k, \deg_x(\eta) + \max_{i=1}^n \deg_x(g_i) - d\}$.
3. *Make an ansatz $f(x) = f_0 + f_1x + \cdots + f_nx^n$ with undetermined coefficients $f_0, \ldots, f_n$ and compute*

   $$p_0(x)f(x) + \cdots + p_r(x)f(x+r) - c_1g_1(x) - \cdots - c_mg_m(x)$$

   with undetermined coefficients $c_1, \ldots, c_m$.
4. *Equate the coefficients of x^i $(i = 0, \ldots, n+d)$ in this polynomial to zero and solve the resulting linear system for $f_0, \ldots, f_n, c_1, \ldots, c_m$. For each solution, return $(f_0 + \cdots + f_nx^n, c_1, \ldots, c_m) \in C[x] \times C^m$.*

Theorem 2.57 *Algorithm 2.56 is correct.* □

Proof It is clear that every output tuple is indeed a solution, that these solutions are linearly independent, and that at least the solutions with $\deg_x(f) \leq n$ must be C-linear combinations of the returned solutions. It therefore suffices to show that there cannot be any solutions with $\deg_x(f) > n$. Indeed, for any choice of $c_1, \ldots, c_m$, the right hand side of the recurrence is a linear combination of $g_1, \ldots, g_m$ and hence a polynomial of degree at most $\max_{i=1}^{m} \deg_x(g_i)$. If $(f, c_1, \dots, c_m) \in C[x]$ is a solution, then we must have $\deg_x \sum_{i=0}^{r} p_i(x) f(x+i) \le \max_{i=1}^{m} \deg_x(g_i)$. By Lemma 2.55, $\deg_x(f) + d - \deg_x(\eta) > \sum_{i=1}^{n} \deg_x(g_i)$ implies that $\deg_x(f)$ is a root of η. The claim follows. ■

In cases where η has large integer roots, it might be better to avoid the classical linear algebra approach used in Algorithm 2.56. As an alternative, we can use the approach of Algorithm 2.51 or the D-finite recurrence for the coefficient sequences of binomial series solutions suggested in Proposition 2.53 above. Doing so requires that we find sequence solutions of inhomogeneous recurrences, which was discussed in Exercises 2 and 3 of Sect. 2.1. Following the approach of Algorithm 2.51, we choose n as in Algorithm 2.56 and compute the first $n + d + 1$ terms of $r + m$ sequence solutions, r solutions forming a basis of the solution space of the homogeneous equation (with 0 as the right hand side) and in addition for each g_i ($i = 1, \dots, m$) one solution where the right hand side is g_i. We compute interpolating polynomials for all of these solutions and then find all C-linear combinations of them whose degree is at most n. The coefficient corresponding to the solution of the inhomogeneous equation with right hand side g_i are exactly the coefficients c_i of the solution tuples.

Example 2.58 Consider the parameterized recurrence

$$(x^2 + x + 1) f(x+1) - (x^2 + 4x + 1) f(x) = c_1(2x^2 + 9x + 8) + c_2(3x^2 + 1).$$

Replacing the right hand side by 0, $2x^2 + 9x + 8$ and $3x^2 + 1$, respectively, we get three sequences, their first six terms together with their corresponding interpolation polynomials are as follows:

n	0	1	2	3	4	5	polynomial
	1	1	2	$\frac{26}{7}$	$\frac{44}{7}$	$\frac{484}{49}$	$-\frac{1}{294}x^5 + \frac{61}{1176}x^4 - \frac{23}{84}x^3 + \frac{1187}{1176}x^2 - \frac{461}{588}x + 1$
	0	8	$\frac{67}{3}$	$\frac{139}{3}$	$\frac{3217}{39}$	$\frac{12125}{91}$	$\frac{11}{1638}x^5 - \frac{671}{6552}x^4 + \frac{469}{468}x^3 + \frac{5087}{6552}x^2 + \frac{20695}{3276}x$
	0	1	$\frac{10}{3}$	$\frac{169}{21}$	$\frac{4306}{273}$	$\frac{17275}{637}$	$\frac{19}{5733}x^5 - \frac{1159}{22932}x^4 + \frac{647}{1638}x^3 - \frac{4913}{22932}x^2 + \frac{9935}{11466}x$

The indicial polynomial for the equation is $x - 3$, so we need to eliminate the terms x^4 and x^5 from the polynomials by linear combination. Since we have three polynomials and only two constraints, it is immediately clear that this will be possible. Note that it is sufficient to consider quintic interpolating polynomials by Lemma 2.50. In fact, we find a solution space of dimension two, generated by

$$\left(\tfrac{6}{13}x^3 + \tfrac{36}{13}x^2 + \tfrac{62}{13}x + \tfrac{77}{39}, 1, 0\right) \quad \text{and} \quad \left(\tfrac{5}{39}x^3 + \tfrac{10}{13}x^2 + \tfrac{4}{39}x + \tfrac{38}{39}, 0, 1\right).$$

□

Let us now turn from polynomial solutions to rational solutions. The problem of finding rational solutions will be reduced to the problem of finding polynomial solutions, which we already know how to handle. Consider a parameterized recurrence equation

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = c_1g_1(x) + \cdots + c_mg_m(x)$$

with known $p_0, \ldots, p_r, g_1, \ldots, g_m \in C[x]$ and unknown $c_1, \ldots, c_m \in C$ and $f \in C(x)$. We may assume that p_0 and p_r are not the zero polynomial. The assumption that the p_i and the g_i are polynomial rather than rational functions is without loss of generality because when they are not, we just need to multiply the whole equation with its common denominator. The search for a rational solution f rather than a polynomial solution is however a significant difference to the setting discussed before, unless somebody tells us the denominator of f. If we know a polynomial $v \in C[x]$ such that there is a solution $(f, c_1, \ldots, c_m) \in C(x) \times C^m$ with $vf \in C[x]$, i.e., where v is (a multiple of) the denominator of f, then we can substitute $f = u/v$ for an unknown polynomial u into the equation, clear denominators, and we obtain a parameterized recurrence equation for u. For every solution $(u, c_1, \ldots, c_m) \in C[x] \times C^m$ of this equation, $(u/v, c_1, \ldots, c_m) \in C(x) \times C^m$ will be a solution of the original equation. The question is thus how to find the possible denominators of rational solutions. By Theorem 2.26, the solution space in $C(x)$ of a linear recurrence is finitely generated. Therefore, for any given equation there exists a finite common denominator for all of its rational solutions. This motivates the following definition.

Definition 2.59 Let $p_0, \ldots, p_r, g \in C[x]$, $p_0, p_r \neq 0$, and let $v \in C[x]$ be such that for every $f \in C(x)$ with

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x)$$

we have $vf \in C[x]$. Then v is called a *universal denominator* or a *denominator bound* for the equation. □

In order to understand how to find a denominator bound for a given equation, let us first see under which circumstances a denominator $v = x - \alpha$ for some $\alpha \in C$ can appear. If we set $f(x) = u(x)/(x-\alpha)$ for unknown $u \in C[x]$ into the equation, we obtain

$$p_0(x)\frac{u(x)}{x-\alpha} + \cdots + p_r(x)\frac{u(x+r)}{x+r-\alpha} = c_1g_1(x) + \cdots + c_mg_m(x).$$

If we multiply this equation by $(x+1-\alpha)(x+2-\alpha)\cdots(x+r-\alpha)$, then all denominators $x+i-\alpha$ for $i > 0$ get canceled, so that all terms except for the first become polynomials. If we bring all the polynomial terms to the right, we see that $p_0(x)u(x)(x+1-\alpha)\cdots(x+r-\alpha)/(x-\alpha)$ must be a polynomial as well. But $x-\alpha$ cannot be a factor of $u(x)$ (otherwise $f(x)$ was a polynomial) and it is coprime with $x+i-\alpha$ for all $i > 0$. It follows that $x-\alpha$ must divide the polynomial $p_0(x)$. Note that this polynomial is part of the input, so we have restricted the possible choices for α to the finitely many roots of $p_0(x)$.

If we multiply the equation above instead by $(x-\alpha)(x+1-\alpha)\cdots(x+r-1-\alpha)$, we can find by an analogous reasoning that $x+r-\alpha$ must divide $p_r(x)$, so the possible choices for α can be restricted further to the finitely many roots of $p_r(x-r)$. In fact, α must be a root of $p_i(x-i)$ for every $i = 0, \dots, r$. The same argument also works when the candidate polynomial $x - \alpha$ is replaced by a power of some fixed irreducible polynomial: a denominator q^n with q irreducible can only appear if $q(x+i)^n \mid p_i(x)$ for all i, and so the possible choices are limited to factors of $\gcd(p_0(x), \dots, p_r(x-r))$.

If a denominator has several distinct irreducible factors, not all of them need to appear among the factors of the $p_i(x)$. For example, the recurrence

$$(x-6)f(x) - (x-2)f(x+1) = 0$$

has the rational solution $f(x) = \frac{1}{(x-3)(x-4)(x-5)(x-6)}$. In this case, the factor $x-6$ of the denominator appears as a coefficient of the equation, and the factor $x-3$ is somehow close to the coefficient $x-2$, but the other factors are missing. Analogous to the observations above, we could expect that the factor $x-4$ of the denominator causes a factor $x-4$ in the coefficient of $f(x)$, but at the same time the factor $x-5$ of the denominator also causes a factor $x-4$ in the coefficient of $f(x+1)$, so that $x-4$ appears in all coefficients and can be canceled from the equation.

In general, if q is an irreducible polynomial such that $q(x)q(x+1)\cdots q(x+s)$ appears in the denominator of a solution but $q(x-1)$ and $q(x+s+1)$ do not, then the trailing coefficient $p_0(x)$ of the recurrence must be a multiple of $q(x)$ and the leading coefficient $p_r(x)$ must be a multiple of $q(x+r+s)$. Comparing the leading and the trailing coefficient allows us to deduce $q(x)$ as well as s. Our goal is to show that all possible factors of the denominator can be recognized in this way.

Definition 2.60 Let $a, b \in C[x]$.

1. $a, b \in C[x]$ are called *shift-equivalent* if there exists $i \in \mathbb{Z}$ such that $a(x) = b(x+i)$.
2. The set $\operatorname{Spread}(a, b) := \{ i \in \mathbb{N} : \gcd(a(x), b(x+i)) \neq 1 \} \subseteq \mathbb{N}$ is called the *spread* of a, b.
3. $a, b \in C[x]$ are called *shift-coprime* if $\operatorname{Spread}(a, b) = \emptyset$.
4. The number $\operatorname{Disp}(a, b) := \max(\operatorname{Spread}(a, b)) \in \mathbb{N} \cup \{-\infty\}$ is called the *dispersion* of a and b. □

Since the greatest common divisor of two polynomials a, b is nontrivial if and only if their resultant is zero (cf. Sect. 1.4), the spread of two polynomials a and b is exactly the set of nonnegative integer roots of the polynomial $\operatorname{res}_x(a(x), b(x+y)) \in C[y]$. Determining the spread and the dispersion thus reduces to finding the integer roots of a polynomial.

Example 2.61

1. For $a = 6x^3 + 37x^2 + 47x + 15$ and $b = 3x^3 - 22x^2 + 44x - 15$, we have

$$\begin{aligned}&\operatorname{res}_x(a(x), b(x+y))\\&= 9(y-5)^2(2y-7)(3y^2-35y+93)(9y^2-90y+116)(12y^2-64y+49).\end{aligned}$$

Therefore, $\operatorname{Spread}(a, b) = \{5\}$ and $\operatorname{Disp}(a, b) = 5$. Indeed, $\gcd(a(x), b(x + 5)) = 3x^2 + 17x + 15$.

2. For $a = 2x + 1$ and $b = x + 2$, we have

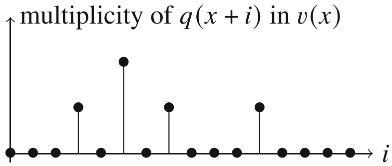
$$\operatorname{res}_x(a(x), b(x+y)) = 2y + 3.$$

As this polynomial has no integer roots, it follows that a and b are shift-coprime.

3. For all $p \in C[x]$, we have $0 \in \operatorname{Spread}(p, p)$. If p is irreducible, then $\operatorname{Spread}(p, p) = \{0\}$. However, $\operatorname{Spread}(p, p) = \{0\}$ does not imply that p is irreducible. For example, we also have $\operatorname{Spread}(x(2x + 1), x(3x + 1)) = \{0\}$. □

The spread of two nonzero polynomials is always a finite set. This is because every nonzero polynomial $a \in C[x]$ has only finitely many monic irreducible factors $q \in C[x]$, and each such factor is coprime with all of its shifts $q(x + i) \in C[x]$ ($i \in \mathbb{Z} \setminus \{0\}$). Since also the nonzero polynomial $b \in C[x]$ only has finitely many factors, there can be at most finitely may $i \in \mathbb{Z}$ with $q(x + i) \mid b(x)$.

In particular, the spread of a polynomial $v \in C[x]$ with itself cannot be infinite. This means that if $q \in C[x]$ is an irreducible factor of v, there are only finitely many $i \in \mathbb{Z}$ such that $q(x + i) \mid v(x)$. In other words, the function which maps $i \in \mathbb{Z}$ to the multiplicity of $q(x + i)$ in $v(x)$ is zero for almost all i.



The polynomials $q(x+i)$ for $i \in \mathbb{Z}$ form an equivalence class in $C[x]$ with respect to shift equivalence. In every equivalence class that contains some factor q of v, there is a unique “right-most” factor and a unique “left-most” factor. The left-most factor is $q(x + i_{\min})$ for $i_{\min} \in \mathbb{Z}$ such that $q(x + i) \nmid v(x)$ for all $i < i_{\min}$, and the right-most factor is defined analogously. Then $i_{\max} - i_{\min} \le \operatorname{Disp}(v, v)$. Moreover, there is some factor with $i_{\max} - i_{\min} = \operatorname{Disp}(v, v)$, because if $s = \operatorname{Disp}(v, v)$, then $\gcd(v(x), v(x + s))$ has a nontrivial factor q, and for this factor we have $q \mid v$ and $q(x - s) \mid v$. Thus, $i_{\max} - i_{\min} \ge s$. The irreducible factors of $\gcd(v(x), v(x + s))$ are therefore right-most factors of v.

The next theorem relates the dispersion $\operatorname{Disp}(v, v)$ of the denominator v of a rational solution to the dispersion of the trailing and the (shifted) leading coefficient of the recurrence.

Theorem 2.62 *Let* $p_0, \dots, p_r, g \in C[x]$, $p_0, p_r \neq 0$, *and let* $f = u/v \in C(x)$ *with* $u, v \in C[x]$ *coprime be such that*

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x).$$

Then $\mathrm{Disp}(v(x), v(x)) \leq \mathrm{Disp}(p_r(x-r), p_0(x))$. □

Proof Let $s = \mathrm{Disp}(v, v)$ and let q be an irreducible factor of $\gcd(v(x), v(x+s))$. By the discussion above, q is a right-most factor of v, which means that $q(x+i) \nmid v(x)$ for all positive integers i. At the same time, $q(x-s)$ is a left-most factor of v in the sense that $q(x-s-i) \nmid v(x)$ for all positive integers i. We show that $q(x) \mid \gcd(p_r(x-r), p_0(x+s))$, so that $s \leq \mathrm{Disp}(p_r(x-r), p_0(x))$, as claimed.

First multiply the equation $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x)$ by $v(x+1)\cdots v(x+r)$ in order to clear the denominators of the terms $p_i(x)f(x+i)$ for all $i > 0$. Then the first term $\frac{p_0(x)u(x)v(x+1)\cdots v(x+r)}{v(x)}$ must be a polynomial, because all other terms of the equation are polynomials. Since $q(x-s)$ is a factor of v, it must be canceled by one of the polynomials in the numerator. It cannot be canceled by u, because u, v are coprime. It can also not be canceled by $v(x+i)$ for any $i = 1, \dots, r$, because $q(x-s) \mid v(x+i)$ would imply $q(x-s-i) \mid v(x)$, which is in conflict with $q(x-s)$ being a left-most factor of v. Therefore, $q(x-s) \mid p_0(x)$ and $q(x) \mid p_0(x+s)$.

Next, multiply the equation $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x)$ by $v(x)\cdots v(x+r-1)$ in order to clear the denominators of the terms $p_i(x)f(x+i)$ for all $i < r$. Then the last term $\frac{p_r(x)v(x)\cdots v(x+r-1)u(x+r)}{v(x+r)}$ on the left hand side must be a polynomial, because all other terms of the equation are polynomials. Since $q(x+r)$ is a factor of $v(x+r)$, it must be canceled by one of the polynomials in the numerator. It cannot be canceled by $u(x+r)$, because u, v are coprime. It can also not be canceled by $v(x+i)$ for any $i = 0, \dots, r-1$, because $q(x+r) \mid v(x+i)$ would imply $q(x+r-i) \mid v(x)$, which is in conflict with $q(x)$ being a right-most factor of v (note that $r - i > 0$ for $i = 0, \dots, r-1$). Therefore, $q(x+r) \mid p_r(x)$ and $q(x) \mid p_r(x-r)$. ■

In the next theorem we give a formula for a denominator bound in terms of the coefficients of the recurrence.

Theorem 2.63 *Let* $p_0, \dots, p_r, g \in C[x]$, $p_0, p_r \neq 0$, *and let* $f = u/v \in C(x)$ *with* $u, v \in C[x]$ *coprime be such that*

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x).$$

Furthermore, let $s = \mathrm{Disp}(v, v)$. *Then* $v(x) \mid \gcd\big(\prod_{i=0}^{s} p_0(x+i), \prod_{i=0}^{s} p_r(x-r-i)\big)$. □

Proof We show that $v(x) \mid \prod_{i=0}^{s} p_0(x+i)$. The proof that $v(x) \mid \prod_{i=0}^{s} p_r(x-r-i)$ is analogous and left as an exercise. Rewrite the recurrence equation in the form

$$f(x) = \frac{1}{p_0(x)}\Bigl(g(x) - \sum_{i=1}^{r} p_i(x) f(x+i)\Bigr).$$

The equation continues to hold when x is replaced by $x+i$ for every $i > 0$. We can therefore apply it repeatedly to rewrite the terms $f(x+i)$ on the right hand side as $C(x)$-linear combinations of $f(x+i+1), \dots, f(x+i+r)$. After s repetitions, we obtain an equation of the form

$$f(x) = \frac{g(x) - \sum_{i=1}^{r} a_i(x) f(x+s+i)}{p_0(x) \cdots p_0(x+s)}$$

with certain $a_1, \dots, a_r \in C[x]$. The denominator of the rational function on the left is $v(x)$ while the denominator on the right is (a divisor of) $p_0(x) \cdots p_0(x+s)v(x+s+1) \cdots v(x+s+r)$. By Theorem 2.62 and the choice of s, we have $\gcd(v(x), v(x+s+i)) = 1$ for $i = 1, \dots, r$. Therefore $v(x) \mid \prod_{i=0}^{s} p_0(x+i)$, as claimed. ■

In principle, the problem of finding rational solutions of linear recurrences with polynomial coefficients is solved at this point: following the advice of Theorem 2.63 we can compute $v(x) = \gcd(\prod_{i=0}^{s} p_0(x+i), \prod_{i=0}^{s} p_r(x-r-i))$ and perform a substitution $f = u/v$ for an unknown polynomial $u \in C[x]$. The problem of finding rational solutions is thus reduced to the problem of finding polynomial solutions.

When s is large, the formula from Theorem 2.63 is not advisable. It would be better to compute a denominator bound without having to expand the two long products in that formula. It is indeed possible to do so, using the following algorithm.

Algorithm 2.64 *(Abramov)*
Input: $p_0, p_r \in C[x] \setminus \{0\}$.
Output: *A denominator bound* $v \in C[x]$ *for linear recurrence equations with polynomial coefficients whose trailing and leading coefficients are* p_0 and p_r, *respectively.*

Set $a(x) = p_r(x-r)$, $b(x) = p_0(x)$ *and* $v(x) = 1$.
Compute $S = \mathrm{Spread}(a(x), b(x)) \subseteq \mathbb{N}$.
while $S \neq \emptyset$ *do*
    Let $s = \max(S)$ *and* $S = S \setminus \{s\}$.
    Let $g(x) = \gcd(a(x), b(x+s))$.
    Let $a(x) = a(x)/g(x)$, $b(x) = b(x)/g(x-s)$ *and*
    $v(x) = v(x) \prod_{k=0}^{s} g(x-k)$.
Return $v(x)$.

Theorem 2.65 *Algorithm 2.64 is correct.* □

Proof According to Theorem 2.63, the polynomial

$$\gcd\Big(\prod_{k=0}^{s} p_0(x+k), \prod_{k=0}^{s} p_r(x-r-k)\Big)$$

is a denominator bound, where $s = \operatorname{Disp}(p_r(x-r), p_0(x))$. We show that right before line 4 we always have $\operatorname{Spread}(a(x), b(x)) \subseteq S$ and that

$$\gcd\Big(\prod_{k=0}^{s} p_0(x+k), \prod_{k=0}^{s} p_r(x-r-k)\Big) = v(x)\gcd\Big(\prod_{k=0}^{\max(S)} b(x+k), \prod_{k=0}^{\max(S)} a(x-k)\Big).$$

By the setup of lines 1 and 2, both assertions are true in the first iteration. Now consider an arbitrary iteration. Let $s_0 = \max(S)$, let $g(x) = \gcd(a(x), b(x+s_0))$, and consider $v_0(x) = \prod_{k=0}^{s_0} g(x-k) = \prod_{k=0}^{s_0} g(x-s_0+k)$.

To show that $\operatorname{Spread}(a(x)/g(x), b(x)/g(x-s_0)) = S \setminus \{s_0\}$, let

$$i \in \operatorname{Spread}(a(x)/g(x), b(x)/g(x-s_0)).$$

Then there is a common divisor of $a(x)/g(x)$ and $b(x+i)/g(x+i-s_0)$, and this divisor must also be a common divisor of $a(x)$ and $b(x+i)$. This shows $i \in S$. At the same time, i cannot be equal to s because if there was a common divisor of $a(x)/g(x)$ and $b(x+s_0)/g(x+s_0-s_0) = b(x+s_0)/g(x)$, then $g(x)$ would not have been the greatest common divisor of $a(x)$ and $b(x+s_0)$.

For the claim about the gcd, observe that

$$\prod_{k=0}^{s_0} b(x+k) = v_0(x)\prod_{k=0}^{s_0}\frac{b(x+k)}{g(x-s_0+k)} \quad\text{and}\quad \prod_{k=0}^{s_0} a(x-k) = v_0(x)\prod_{k=0}^{s_0}\frac{a(x-k)}{g(x-k)},$$

so

$$\begin{aligned} &v(x)\gcd\Big(\prod_{k=0}^{s_0} b(x+k), \prod_{k=0}^{s_0} a(x-k)\Big)\\ &\quad = v(x)v_0(x)\gcd\Big(\prod_{k=0}^{s_0}\frac{b(x+k)}{g(x-s_0+k)}, \prod_{k=0}^{s_0}\frac{a(x-k)}{g(x-k)}\Big). \end{aligned}$$

As shown in Exercise 22, the gcd on the right hand side does not change if the upper bound is replaced by the dispersion of $b(x)/g(x-s_0)$ and $a(x)/g(x)$, which, as we have shown above, is smaller than s_0. This completes the proof of the loop invariant.

Once the loop terminates, we have $\operatorname{Spread}(a(x), b(x)) = \emptyset$, so

$$\gcd\Big(\prod_{k=0}^{s} b(x+k), \prod_{k=0}^{s} a(x-k)\Big) = 1$$

for all $s \in \mathbb{N}$. The correctness of the algorithm follows. ■

Example 2.66 Consider the recurrence

$$\begin{aligned}&(x-1)x(x+2)(2x+1)f(x)\\&\quad-(x+1)(2x+3)(5x^2+11x+4)f(x+1)\\&\quad+2(x+1)(x+2)(2x+3)(2x+5)f(x+2)=0.\end{aligned}$$

With $a(x)=2(x-1)x(2x-1)(2x+1)$ and $b(x)=(x-1)x(x+2)(2x+1)$ we get $\operatorname{Spread}(a(x),b(x))=\{0,1\}$.

For $s=1$ we get $g(x)=\gcd(a(x),b(x+1))=x$, which gives a contribution of $x(x-1)$ to the denominator bound. After clearing the factors, we are left with $a(x)=(x-1)(2x-1)(2x+1)$ and $b(x)=x(x+2)(2x+1)$.

In the next iteration, with $s=0$, we get $g(x)=\gcd(a(x),b(x))=2x+1$, which gives a contribution of $2x+1$ to the denominator bound. The final result is thus $v(x)=x(x-1)(2x+1)$.

Applying the substitution $f(x)=u(x)/v(x)$ and clearing denominators turns the recurrence into

$$x(x+2)u(x)-(5x^2+11x+4)u(x+1)+2x(2x+3)u(x+2)=0.$$

The solution space of this recurrence in $C[x]$ is generated by $x-1$. Consequently, the solution space of the original recurrence in $C(x)$ is generated by $\frac{x-1}{x(x-1)(2x+1)}=\frac{1}{x(2x+1)}$. We see that the denominator bound contains a superfluous factor $x-1$. □

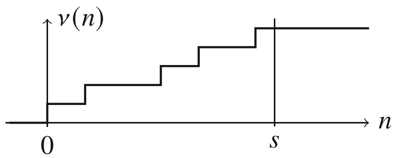
Abramov's algorithm is easy to implement but, as shown in the example above, it does not necessarily return the smallest possible universal denominator. This behavior is not surprising in view of the fact that it only looks at the leading and the trailing coefficient of the recurrence but disregards all the intermediate coefficients. We now discuss an alternative algorithm which also takes the intermediate coefficients of the recurrence into account. Although the description of that algorithm is more lengthy, it is not necessarily more difficult.

In order to simplify the discussion, let us assume that C is algebraically closed, so that every monic irreducible polynomial has the form $x-\alpha$ for some $\alpha\in C$. We can then talk more conveniently about the poles of rational solutions rather than about the factors of their denominators. Instead of shift-equivalent factors, we can talk about poles with integer distance. We call two elements of C equivalent if their difference is an integer, and we write $C/\mathbb{Z}$ for the set of equivalence classes. For every equivalence class $\alpha+\mathbb{Z}$, we seek a function $\nu\colon\alpha+\mathbb{Z}\to\mathbb{N}$ such that $\nu(\alpha+k)=j$ means that the pole $\alpha+k$ has multiplicity at most j in any rational solution of the equation at hand. Theorem 2.63 implies that only finitely many equivalence classes can contribute to the denominator, say $\alpha_1+\mathbb{Z},\dots,\alpha_m+\mathbb{Z}$ with $\alpha_i-\alpha_j\notin\mathbb{Z}$ for $i\neq j$. For all other equivalence classes, we can choose ν identically zero. Theorem 2.63 also implies that for every equivalence class $\alpha_i+\mathbb{Z}\to\mathbb{N}$, there is a function $\nu_i:\alpha_i+\mathbb{Z}$ with $\nu_i(\alpha_i+k)=0$ for almost all $k\in\mathbb{Z}$. With any selection of such functions ν_i, the polynomial $\prod_{i=1}^{m}\prod_{k\in\mathbb{Z}}(x-(\alpha_i+k))^{\nu_i(\alpha_i+k)}$ is a denominator bound.

For every $\alpha \in C$, the leftmost element of $\alpha+\mathbb{Z}$ at which a rational solution can possibly have a pole is the leftmost root of $p_0(x)$ in $\alpha+\mathbb{Z}$. The rightmost element of $\alpha+\mathbb{Z}$ at which there can be a pole is the rightmost root of $p_r(x-r)$ in $\alpha+\mathbb{Z}$. These observations are again consequences of Theorem 2.63. The question is what happens in between. By applying a suitable change of variables $x = x-\alpha+k$ with $k \in \mathbb{Z}$ to the recurrence equation at hand, we can consider the equivalence class $\mathbb{Z}$ instead of $\alpha+\mathbb{Z}$, and we may assume that the leftmost candidate for a pole of a rational solution is 0. If $v \in C(x)$ is a rational solution of the recurrence, then $v(x+q) \in C(q)(x)$ is a solution of the deformed recurrence (cf. Definition 2.18), and then also the sequence $(v(n+q))_{n=0}^{\infty}$ is a solution of the deformed recurrence. Recall from the discussion in Sect. 2.2 that $v(n+q)$ is well defined for every $n \in \mathbb{N}$, and that the multiplicity of q in the denominator of $v(n+q) \in C(q)$ is exactly the multiplicity of $x-n$ in the denominator of $v \in C(x)$.

Consider a basis $\{b_1,\dots,b_r\}$ of sequence solutions in $C((q))^{\mathbb{Z}}$ of the deformed recurrence whose initial values are chosen such that $b_i(-j) = \delta_{i,j}$ for $i, j = 1,\dots,r$. As we have set things up to ensure that a rational solution v cannot have poles at $n = -1,-2,\dots,-r$, we can identify any such solution with a certain $C[[q]]$-linear combination of $b_1,\dots,b_r$. Then the order of a pole of v at any point $x = n$ is bounded by the orders of the poles of $b_1,\dots,b_r$ at n. Consider the function $\nu\colon \mathbb{Z} \to \mathbb{N}$ which maps every $n \in \mathbb{N}$ to the smallest $k \in \mathbb{N}$ such that $q^k b_i(n)$ is a power series for every $i = 1,\dots,r$. Actually, we may allow k to be negative when each $b_i(n)$ $(i = 1,\dots,r)$ is a power series of positive order. If k is negative, it means that the polynomial $(x-\alpha-n)^{-k}$ must divide the numerator of any rational solution.

Negative values of k appear only in very special circumstances. Typically ν will be an increasing function which is constant 0 for $n < 0$ and also constant for values n beyond the largest possible pole position:



Such a function is not useful for our purpose because we need to have $\nu(n) = 0$ for almost all $n \in \mathbb{Z}$. A simple way to achieve this is to simply redefine $\nu(n) := 0$ for $n > s$, because we already know that a rational solution cannot have any poles there.

There is a better way. We can exploit the fact that rational solutions can only correspond to sequences $b \in C((q))^{\mathbb{Z}}$ with $b(n) \in C[[q]]$ for $n = s,\dots,s+r-1$, because rational solutions cannot have poles for $n \geq s$. We can thus make an ansatz $b = \alpha_1 b_1 + \cdots + \alpha_r b_r$ with undetermined coefficients $\alpha_1,\dots,\alpha_r$ and then equate the coefficients of the terms q^k with $k < 0$ in $b(n)$ for $n = s,\dots,s+r-1$ to zero.

This gives a linear system for $\alpha_1, \dots, \alpha_r$ over C, the solutions of which translate into a basis of the space of b's. If $\tilde{b}_1, \dots, \tilde{b}_t$ is such a basis, then we can define $\nu\colon \mathbb{Z} \to \mathbb{N}$ as the function which maps every $n \in \mathbb{N}$ to the smallest $k \in \mathbb{N}$ such that $q^k \tilde{b}_i(n)$ is a power series for $i = 1, \dots, t$.

There is an even better way. We can exploit the fact that rational solutions cannot correspond to sequences $b \in C((q))^{\mathbb{Z}}$ with $b(n) \in qC[[q]]$ for $n = s, \dots, s+r-1$, because for such sequences the recurrence would force $b(n) \in qC[[q]]$ for all $n > s$, so such a sequence would correspond to a rational function with infinitely many roots, which does not exist. If V denotes the C-vector space generated by $\tilde{b}_1, \dots, \tilde{b}_r$ from before, we can determine a basis of the subspace $U \subseteq V$ consisting of all C-linear combinations v of $\tilde{b}_1, \dots, \tilde{b}_r$ with $v(n) \in qC[[q]]$ by making an ansatz, equating the coefficients of q^0 to zero and solving a linear system. If $W \subseteq V$ is a complementary space of U in V, i.e., if we have $V = U \oplus W$ as C-vector spaces, then any rational solution must correspond to an element of W, so if $w_1, \dots, w_d \in C((q))^{\mathbb{Z}}$ form a basis of W, we can define $\nu\colon \mathbb{Z} \to \mathbb{N}$ as the function which maps every $n \in \mathbb{N}$ to the smallest $k \in \mathbb{N}$ such that $q^k w_i(n) \in C[[q]]$ for $i = 1, \dots, d$.

Another possible improvement consists of computing an additional function $\tilde{\nu}$, defined analogously to ν but using the recurrence in the reverse direction, and then taking the minimum of $\tilde{\nu}$ and ν. We leave it to the creativity of the reader to come up with further optimizations and formulate the algorithm in a general form which leaves space for such additional improvements.

Algorithm 2.67 *(van Hoeij)*
Input: $p_0, \dots, p_r, g \in C[x]$ *with* $p_0, p_r \neq 0$.
Output: *A rational function* $v \in C(x)$ *such that whenever* $f \in C(x)$ *is such that*

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x),$$

then $vf \in C[x]$.

Let $v = 1$.
for all $\alpha \in \bar{C}$ *with* $p_r(\alpha - r) = 0$ *and* $p_r(\alpha - i - r) \neq 0$ *for all integers* $i > 0$ *do*
  Let $s \in \mathbb{N}$ *be maximal such that* $\alpha + s$ *is a root of* p_0. *If no such* s *exists, go straight to the next* α.
  Set $\tilde{p}_i(x) = p_i(x + q - \alpha) \in C(\alpha)(q)[x]$ *for* $i = 0, \dots, r$ *and* $\tilde{g}(x) = g(x + q - \alpha)$.
  for $i = 1, \dots, r$ *do*
    Define the sequence $b_i \in C((q))^{\mathbb{Z}}$ *by* $b_i(-j) = \delta_{i,j}$ *for* $j = 1, \dots, r$, *let*

$$\tilde{p}_i(n)b_i(n) + \cdots + \tilde{p}_r(n)b_i(n+r) = \tilde{g}(n)$$

for $n \in \mathbb{Z}$, *and let* $V \subseteq C((q))^{\mathbb{Z}}$ *be the* $C[[q]]$*-module generated by* $b_1, \dots, b_r$.

7 *Find a basis* $\tilde{b}_1, \ldots, \tilde{b}_t$ *of some* $C[[q]]$*-submodule* W *of* V *for which it is ensured that every rational solution of the recurrence corresponds to an element of* W.

8 *Set* $v(x) = v(x)\prod_{n=0}^{s}(x-\alpha-n)^{\nu(n)}$ *where* $\nu(n)$ *is the minimal* $k \in \mathbb{Z}$ *such that* $q^k\tilde{b}_j(n) \in C[[q]]$ *for* $j = 1, \ldots, t$.

9 *Return* $v(x)$.

Theorem 2.68 *Algorithm 2.67 is correct.* □

Proof Suppose otherwise. Then there is a recurrence $p_0(x)f(x)+\cdots+p_r(x)f(x+r) = g(x)$ which has a rational solution $f(x) \in C(x)$ for which $v(x)f(x)$ is not a polynomial, where $v(x) \in C(x)$ is the output of the algorithm. Fix such a recurrence and such a rational solution.

If vf is not a polynomial, it must have at least one pole. This pole must be a pole of v or a pole of f. Either way, by the construction of v and because of Theorem 2.63, such a pole can only appear at points $\alpha + m \in \bar{C}$ for some left-most root α of $p_r(x-r)$ and some $m \in \{0, \ldots, s\}$. Fix such an α and such an m.

The rational function $\tilde{f}(x) = f(x+q-\alpha) \in C(\alpha)(q)(x)$ is such that $\tilde{p}_0(x)\tilde{f}(x) + \cdots + \tilde{p}_r(x)\tilde{f}(x+r) = \tilde{g}(x)$ for $\tilde{p}_0, \ldots, \tilde{p}_r, \tilde{g}$ as defined in line 4 in the iteration for the fixed α.

As $\tilde{f}(x)$ has no poles in $\mathbb{Z}$ (because $q \notin C$), we can identify it with an element of $C((q))^{\mathbb{Z}}$, and by the assumption on W in line 7, $(\tilde{f}(n))_{n=0}^{\infty}$ must be a $C[[q]]$-linear combination of $\tilde{b}_1, \ldots, \tilde{b}_t$.

If f has a pole of order k at $\alpha + m$, then the smallest exponent of q appearing in $\tilde{f}(m) \in C((q))$ is k, and then at least one b_j must involve a power of q with exponent k or less. Hence we have $\nu(m) \geq k$ in line 8 and so vf has no pole at $\alpha + m$.

There remains the possibility that v has a pole of order k at $\alpha + m$. In this case, we have $\nu(m) = -k$ in line 8. By definition of ν, this means that all b_j only involve powers of q with exponent k or more. Since $\tilde{f}$ is a $C[[q]]$-linear combination of the $b^{(j)}$'s, it follows that also $\tilde{f}(m) \in C((q))$ can only involve powers of q with exponent k or more. But then f has a root of order at least k at $\alpha+m$, so also in this case vf has no pole at $\alpha + m$. ■

In an implementation of Algorithm 2.67 we will represent the terms $b_i(n), \tilde{b}_i(n) \in C((q))$ by truncated series. The truncation order of the initial terms must be chosen large enough so that the correctness is not affected. If W is chosen as described in the paragraphs before the algorithm and we restrict to nonnegative values of k, then it is sufficient take the sum of the multiplicities of the integer roots of p_r.

We will also want to avoid computing in algebraic extension fields $C(\alpha)$, especially since all we really need in line 8 are the orders of certain series, rather than their coefficients. Therefore, in order to handle an irrational root $\alpha \in A$, it is a good idea to search for a prime $p \in \mathbb{Z}$ such that the minimal polynomial $m \in C[x]$ of α has a root in $\mathbb{Z}_p$ when viewed as element of $\mathbb{Z}_p[x]$. Then we can map α to this root and do the computations in lines 4–7 with $\mathbb{Z}_p$ in place of $C(\alpha)$. In the unlikely event that this leads to a division by zero, we try again with another prime p. In line 8, we will then use $m(x-n)$ instead of $x-\alpha-n$.

Example 2.69

1. Consider the recurrence

$$(x-2)(4x^2+3x-9)f(x)-(x+1)(16x^3-16x^2-65x+64)f(x+1)$$
$$+4(x+1)(x+2)(4x^2-5x-8)f(x+2)=0.$$

The only relevant equivalence class is $\mathbb{Z}$, because for the roots α of $4(x-2)^2-5(x-2)-8$, no suitable $s\in\mathbb{N}$ is found in line 3. In the class $\mathbb{Z}$, the leftmost possible position of a pole is $x=0$ and the rightmost possible position is $x=2$. We have the following basis of the solution space in $C((q))^{\mathbb{Z}}$ (we omit the truncation indicator "$+\cdots$" due to lack of space):

n	-2	-1	0	1	2	3	4
$b_1(n)$	1	0	$-\frac{2}{q}-\frac{19}{2}$	$\frac{14}{q}+\frac{49}{2}$	$-\frac{13}{q}+\frac{3}{4}$	$\frac{1}{3q}-\frac{217}{36}$	$-\frac{1}{12q}-\frac{71}{36}$
$b_2(n)$	0	1	$\frac{1}{q}+\frac{15}{2}$	$-\frac{13}{q}-\frac{23}{2}$	$\frac{25}{2q}-13$	$-\frac{1}{6q}+\frac{109}{18}$	$\frac{1}{24q}+\frac{569}{288}$

Neither of the two basis elements can correspond to a rational solution, because rational solutions cannot have poles at $n=3$ or $n=4$. The C-vector space generated by b_1,b_2 in $C((q))^{\mathbb{Z}}$ consisting of all sequences whose terms at $n=3$ and $n=4$ are power series is one dimensional. It is generated by $b_3:=b_1+2b_2$. We have

n	-2	-1	0	1	2	3	4
$b_3(n)$	1	2	$\frac{11}{2}$	$-\frac{12}{q}+\frac{3}{2}$	$\frac{12}{q}-\frac{101}{4}$	$\frac{73}{12}$	$\frac{95}{48}$

The orders of $b_3(n)$ for $n=0,1,2$ imply the denominator bound $(x-1)(x-2)$. Since the equation has the rational solution $\frac{1}{(x-1)(x-2)}$, this bound is optimal. Abramov's algorithm returns the suboptimal bound $x(x-1)(x-2)$.

2. Applying the same calculation to the recurrence

$$(x-1)x(2x^2+2x-1)f(x)+4x^2(x+1)f(x+1)$$
$$-(x+1)(x+2)(2x^2-2x-1)f(x+2)=0$$

leads to the denominator bound $v(x)=x(x-1)(x-2)$. However, the solution space in $C(x)$ is again generated by $\frac{1}{(x-1)(x-2)}$, which shows that also Algorithm 2.67 does not necessarily find the smallest possible denominator bound. ◻

Exercises

1. Let $f(x) = \sum_{i=0}^{n} a_i \binom{x}{i}$ be a polynomial. Show that $a_n = \sum_{k=0}^{n} (-1)^{n+k} \binom{n}{k} f(k)$.

Hint: The identity $\binom{n-k}{i}\binom{n}{k} = \binom{n}{i}\binom{n-i}{k}$ might be handy.

2. Determine the coefficient of S_n^0 in the operator $S_n^d M$ from the proof of Proposition 2.53.

3. Show that every polynomial $p \in C[x]$ is a solution of a homogeneous linear recurrence with polynomial coefficients.

4. How could you see by inspection (i.e., without using a computer or even pen and paper) that the recurrence

$$(2x^2 + 5x - 3)f(x+3) - (2x^2 - 2x + 5)f(x+2)$$
$$+ (3x^2 - 5x + 2)f(x+1) + (8x^2 - 6x + 5)f(x) = 0$$

has no polynomial solutions?

5. Find all solutions in $\mathbb{Q}[x]$ of the following recurrences:

a. $f(x+4) + f(x+3) - 3f(x+2) - f(x+1) + 2f(x) = 0$;
b. $(x+1)f(x+2) - (x+6)f(x+1) - 8f(x) = 0$;
c. $(x-3)(x+2)f(x+2) - (3x^2+x-22)f(x+1) + 2(x-2)(x+5)f(x) = 0$;
d. $(x+6)(x+9)f(x+2) - (3x^2+41x+118)f(x+1) + 2(x+1)(x+10)f(x) = 0$.

6. Find all solutions in $\mathbb{Q}[x] \times \mathbb{Q}^m$ of the following parameterized recurrences:

a. $(x+6)(x+9)f(x+2) - (3x^2+41x+118)f(x+1) + 2(x+1)(x+10)f(x) = c_1(8 + 16x + x^2) + c_2(7x + x^2)$;
b. $f(x) = c_1(8 + 16x + x^2) + c_2(7x + x^2)$;
c. $(x+1)^2 f(x+1) + (x+5)^2 f(x) = c_1(1 + x + x^2) + c_2(1 + 2x + 3x^2)$;
d. $(x+1)f(x+1) - (x+5)f(x) = c_1(1 + x + x^2)$.

7. Find all values of α for which the recurrence

$$(x+2)(\alpha + 2x^2 + 11x)f(x) + 2(3x^2 + 12x + 16)f(x+1)$$
$$-(x+1)(2x^2 + 7x + 14)f(x+2) = 0$$

has a polynomial solution.

8. Let $p_0, \dots, p_r \in C[x]$ be of degree at most 1, and let $g_1, g_2 \in C[x]$ be of degree at most 3. Show that the parameterized recurrence $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = c_1 g_1(x) + c_2 g_2(x)$ has a nontrivial solution in $C[x] \times C^2$.

9. Let K be a difference field containing $C(x)$ with $\operatorname{Const} K = C$. Consider a linear recurrence equation with coefficients in K. How can we find its solutions in $C(x)$?

10*. Let K be a difference field containing $C(x)$ with $\operatorname{Const} K = C$. Consider a parameterized recurrence equation with coefficients in $C(x)$ and right hand side in K. How can we find its solutions in $C(x) \times C^m$?

11. Design an algorithm which finds all solutions of the form $p(x)\phi^x$ with $p \in C[x]$ and $\phi \in C$ of a given homogeneous linear recurrence with polynomial coefficients.

12. Let $(a_n)_{n=0}^{\infty}$ be defined by $a_0 = 5$, $a_1 = 2$, and

$$(n-2)na_n - (2n^2 - 10n + 3)a_{n+1} + (n-5)(n-3)a_{n+2} = 0$$

for $n \in \mathbb{N}$. Find a closed form for a_n.

13*. Show that for all $p(x) \in C[x]$ there exists a $q(x) \in C[x]$ such that $\sum_{k=0}^{n} p(k) = q(n)$ for all $n \in \mathbb{N}$.

14. Prove or disprove: if $f, p_0, \ldots, p_r \in C[x]$ are such that $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = 0$ and $\deg_x(f) > r$ and f is irreducible, then $f \mid p_r$.

15. Show that for all $r, k \in \mathbb{N}$ with $k \leq r$ there is a recurrence of order r whose solution space in $C[x]$ has dimension k.

16. Show that if $p(x) \in C[x]$ is irreducible then so is $p(x+i)$ for every $i \in \mathbb{Z}$.

17. Show that if $p(x), q(x) \in C[x]$ are shift-coprime, then so are $p(x+i)$ and $q(x+j)$ for all $i, j \in \mathbb{Z}$.

18. Determine $\operatorname{Spread}((x-3)(x-5)(2x-3)(2x-4)(3x+1)(3x+2), (x-5)(x-8)(2x+3)(3x+5)(4x+7))$.

19. Show that for all $a, b, c \in C[x]$ we have $\operatorname{Spread}(a, bc) = \operatorname{Spread}(a, b) \cup \operatorname{Spread}(a, c)$.

20. Show that $\operatorname{Spread}(a(x+k), b(x+k)) = \operatorname{Spread}(a(x), b(x))$ for all $a, b \in C[x]$ and all $k \in \mathbb{Z}$.

21.** With the notation of Theorem 2.63, show that $v(x) \mid \prod_{i=0}^{s} p_r(x-r-i)$.

22. Let $u, v \in C[x]$ and $s = \operatorname{Disp}(v, u)$. Show that $\gcd(\prod_{k=0}^{s} v(x-k), \prod_{k=0}^{s} u(x+k)) = \gcd(\prod_{k=0}^{n} v(x-k), \prod_{k=0}^{n} u(x+k))$ for every $n \geq s$.

23. Find all solutions in $\mathbb{Q}(x)$ of the following recurrences:
a. $(x-5)(x-4)(2x-5)(4x-1)f(x) - (x-4)(4x-3)(4x^2-6x+5)f(x+1) + (x-1)(x+1)(2x+1)(4x-5)f(x+2) = 0$;
b. $(x+1)(x^2+7x+9)f(x) - (2x^3-9x^2+3x-7)f(x+1) + (x+5)(x^2+5x+3)f(x+2) = 0$;
c. $x(2x-5)(2x+1)f(x) - (2x-1)(4x^2-4x+3)f(x+1) + (x-1)(2x-1)(2x+1)f(x+2) = 0$;
d. $22(3x+1)(x-4)^2 f(x) - (321x^3 - 1111x^2 - 2337x + 6935)f(x+1) + 85x(3x+16)(x-4)f(x+2) = 0$.

24. Find all solutions in $\mathbb{Q}(x) \times \mathbb{Q}^m$ of the following parameterized recurrences.

a. $3(x+1)f(x)-2(x+3)f(x+1)-(x+5)f(x+2) = c_1+c_2\frac{1}{x+3}+c_3\frac{1}{x+4}$;

b. $(x+1)(x+2)f(x)-2x(x+2)f(x+1)+(x-9)(x+4)f(x+2) = c_1+c_2x$.

25. Show that $H_n = \sum_{k=1}^{n} \frac{1}{k}$ is not rational.

26. Consider a linear recurrence equation with polynomial coefficients for an unknown function f. Let η be its indicial polynomial and let v be a denominator bound for the equation. Let $\tilde{\eta}$ be the indicial polynomial of the recurrence for $\tilde{f} = f/v$. How are η and $\tilde{\eta}$ related?

27. Let $p_0, \dots, p_r, g, h \in C[x]$, $p_0, p_r \neq 0$. Prove or disprove: every denominator bound for $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = g(x)$ is also a denominator bound for $p_0(x)f(x) + \cdots + p_r(x)f(x+r) = h(x)$.

28***.** Consider the following recurrence:

$$
\begin{aligned}
&(x-6)(x-5)(x^3-9x^2+24x-22)f(x)\\
&-(x-5)(x-3)(x^4-11x^3+37x^2-44x+8)f(x+1)\\
&+(x-3)(x-2)(x-1)(x^3-12x^2+45x-56)f(x+2) = 0.
\end{aligned}
$$

Construct a function $\nu\colon \mathbb{Z} \to \mathbb{Z}$ which bounds the multiplicities of integer poles in the range $0, \dots, 10$ for rational function solutions of this recurrence **a.** by passing through the range from left to right, **b.** by passing through the range from right to left, **c.** by passing through the range from left to right and considering only the subspace of sequences that has no poles right after the range.

29***.** For a certain equivalence class $\alpha + \mathbb{Z} \subseteq C$, what is the function $\nu\colon \mathbb{Z} \to \mathbb{Z}$ such that $\prod_{n\in\mathbb{Z}}(x-\alpha-n)^{\nu(n)}$ gives the contribution of $\alpha + \mathbb{Z}$ to Abramov's denominator bound?

30***.** Abramov's algorithm uses the nonnegative integers i with $\gcd(p_r(x-r), p_0(x+i)) \neq 1$ in order to deduce information about the possible denominators of a rational solution. Show that for equations of order $r = 1$, we can obtain some information about the possible numerators from the negative integers i with $\gcd(p_r(x-r), p_0(x+i)) \neq 1$.

31. The notions introduced in Definition 2.60 are used more generally for any automorphism $\sigma\colon C[x] \to C[x]$ rather than just the specific automorphism defined by $\sigma(p(x)) = p(x+1)$. Consider the automorphism defined by $\sigma(p(x)) = p(2x)$. Determine $\operatorname{Spread}((x+3)(16x+1), x(x-1)(2x+1))$ and $\operatorname{Spread}(x(x+1), x(x-1))$ with respect to σ.

References

Algorithms for finding polynomial or rational solutions of linear recurrence equations are more recent than the corresponding algorithms in the differential case discussed in Sect. 3.5. The basic ideas are similar, but in the recurrence case, it takes some more effort to make them work. Fast algorithms based on factorial series were proposed by Abramov, Bronstein, and Petkovšek [21] and further improved by Bostan, Chyzak, Cluzeau, and Salvy [81]. In order to be able to offer algorithms that take less time than the output can be long, they return the solutions in a compressed format.

Abramov [3, 4] gave the first algorithm for finding rational solutions, generalizing his own pioneering work on rational summation [2]. He also introduces the notions of spread and dispersion. Gerhard [208] gives fast algorithms for computing spread and dispersion. The justification of Abramov's algorithm presented in this section is due to Chen, Paule and Saad [133]. Van Hoeij's algorithm for finding rational solutions appeared in [444]. A noteworthy difference between Algorithm 2.64 and 2.67 is that Abramov's algorithm only takes the leading and the trailing coefficient of the recurrence into account, while van Hoeij's algorithm also uses the intermediate coefficients. Hou and Mu [241] showed that Abramov's algorithm is optimal in the sense that every correct denominator bounding algorithm which can find sharper bounds than Abramov's algorithm must use more than just the leading and the trailing coefficient.

More general algorithms for solving linear difference equations allow the coefficients of the given equation to belong to some difference field K and ask for solutions in the same field. The situation considered here corresponds to the choice $K = C(x)$ with the shift $\sigma: K \to K$ defined through $\sigma(x) = x + 1$. Bronstein [113] and Schneider [385, 387] develop such algorithms for certain types of difference fields K. Although technically more involved, their algorithms also rely on the strategies of finding degree bounds and denominator bounds. New ideas are needed if we also want to find solutions that do not belong to K. This is the topic of the next section.

2.6 Hypergeometric and d'Alembertian Solutions

Consider a first order equation $u(x)f(x) - v(x)f(x+1) = 0$ with $u, v \in C[x]\setminus\{0\}$. If this equation does not have a solution in $C(x)$, we can construct a difference field extension in which it does have a solution. Take the field $E = C(x, y)$ of rational functions in two variables and define $\sigma: E \to E$ via $\sigma(r(x, y)) = r(x+1, \frac{u}{v}y)$ for all $r \in C(x, y)$. Then E is a difference field extension of $C(x)$ which contains an additional element y for which the shift is defined in such a way that $uy - v\sigma(y) = 0$. In other words, y is a solution of the recurrence we started with.

Definition 2.70 Let K be a difference field and let E be a difference field extension of K. An element $y \in E \setminus \{0\}$ is called *hypergeometric* over K if $\sigma(y)/y \in K$. □

We are usually interested in the case when K is the rational function field $C(x)$. If this is the case, we will drop the reference to K.

Example 2.71

1. Every nonzero element y of the ground field $K \subseteq E$ is hypergeometric, because for all $y \in K$ we have $\sigma(y) \in K$ and therefore also $\sigma(y)/y \in K$. In particular, when $K = C(x)$, all rational functions are hypergeometric.
2. Exponentials ϕ^x with $\phi \in C$ are hypergeometric, because $\phi^{x+1}/\phi^x = \phi \in C \subseteq K$.
3. Further typical hypergeometric expressions include factorials like $x!$, $(3x+5)!$, $\frac{1}{x!}$, and binomials like $\binom{2x}{x}$, $\binom{x+3}{x-1}$, $1/\binom{2x}{x}$. For example, we have $(x+1)!/x! = x+1 \in C(x)$ and $\binom{2(x+1)}{x+1}/\binom{2x}{x} = 2(2x+1)/(x+1) \in C(x)$.
   Note that by $x!$ we do not mean the sequence $(n!)_{n=0}^{\infty}$. The meaning instead is as follows. Consider the difference field $E = C(x, y)$ defined by by $\sigma(r(x, y)) = r(x+1, (x+1)y)$. Then $x!$ is only a convenient notation for the element $y \in E$, which helps us remember how the shift action is defined. This notational convention allows us to write down difference fields without explicitly defining the shift operation: the shift operation acting on $E = C(x, x!)$ is simply the one which is suggested by the notation used for the generators.
4. The object 2^{x^2} is not hypergeometric over $C(x)$, but it is hypergeometric over $C(2^x)$, because $2^{(x+1)^2}/2^{x^2} = 2^{2x+1} = 2\,(2^x)^2 \in C(2^x)$. □

The product of two hypergeometric terms is again hypergeometric, because if $u_1 y_1 - v_1\sigma(y_1) = 0$ and $u_2 y_2 - v_2\sigma(y_2) = 0$, then $u_1u_2(y_1y_2) - v_1v_2\sigma(y_1y_2) = 0$. Also the reciprocal of a hypergeometric term is again hypergeometric. In contrast, the sum of two hypergeometric terms is in general not hypergeometric. For example, although 1 and 2^x are both hypergeometric, $1 + 2^x$ is not. The sum of two hypergeometric terms y_1 and y_2 is hypergeometric if and only if the quotient y_1/y_2 is a rational function (Exercise 3). In this case, the terms y_1 and y_2 are called *similar*. Similarity is an equivalence relation on the set of hypergeometric terms. Its equivalence classes together with zero are $C(x)$-vector spaces, i.e., if y_1 and y_2 are similar and y_3 is a $C(x)$-linear combination of y_1 and y_2, then either y_3 is zero or y_1 and y_2 are similar to y_3. The equivalence classes are also closed under shift, because every hypergeometric term y is similar to $\sigma^i(y)$ for all $i \in \mathbb{Z}$.

For these reasons, given $p_0, \ldots, p_r \in C[x]$ and a hypergeometric term y, we have that $p_0 y + p_1\sigma(y) + \cdots + p_r\sigma^r(y)$ is either zero or similar to y. We are interested here in the situation where the result is zero. In this case, the hypergeometric term y is a solution of the recurrence

$$p_0(x)f(x) + \cdots + p_r(x)f(x+r) = 0.$$

Given such a recurrence equation, our goal is to find all of its hypergeometric solutions. To find a hypergeometric solution means to find a rational function $u/v \in C(x)$ such that the term y defined by $\sigma(y) = \frac{u}{v}y$ is a solution to the equation.

We will discuss two algorithms. The first is based on an analysis of possible cancellations, similar to Abramov's algorithm for finding rational solutions. Suppose that y is a hypergeometric solution of the recurrence above, and let $u, v \in C[x]$ be such that $\sigma(y)/y = u/v$. If we plug y into the left hand side of the equation, we obtain

$$p_0 y + p_1\sigma(y) + \cdots + p_r\sigma^r(y) = \Big(p_0 + p_1\frac{u}{v} + \cdots + p_r\frac{u\sigma(u)\cdots\sigma^{r-1}(u)}{v\sigma(v)\cdots\sigma^{r-1}(v)}\Big)y.$$

This expression is zero if and only if the rational function in the parentheses is zero. After multiplying this rational function by $v\sigma(v)\cdots\sigma^{r-1}(v)$, we get a polynomial expression involving two unknowns u and v. In this expression, all terms except the first contain u, so also the first term must be a multiple of u. Likewise, all terms except the last contain $\sigma^{r-1}(v)$, so also the last term must be a multiple of $\sigma^{r-1}(v)$. We thus have the two conditions

$$u \mid p_0 v\sigma(v)\cdots\sigma^{r-1}(v) \quad \text{and} \quad \sigma^{r-1}(v) \mid p_r u\sigma(u)\cdots\sigma^{r-1}(u).$$

We are free to assume without loss of generality that u and v are coprime, because all we are really interested in is the quotient u/v, so we may discard the factors v and $\sigma^{r-1}(u)$ on the right hand sides. But this does not help too much. It is still possible that there is a nontrivial common factor between u and some $\sigma^i(v)$, or between $\sigma^{r-1}(v)$ and some $\sigma^i(u)$, so we are not entitled to assume that u must divide p_0 and that $\sigma^{r-1}(v)$ must divide p_r.

Suppose that u and $\sigma^i(v)$ share a nontrivial common factor q. Then we can write $u = q\bar{u}$ and $v = \sigma^{-i}(q)\bar{v}$ for some polynomials $\bar{u}, \bar{v}$. Any hypergeometric term y with $\sigma(y)/y = u/v$ can then be viewed as the product $y = r\bar{y}$ of two hypergeometric terms $r, \bar{y}$ with $\sigma(r)/r = q/\sigma^{-i}(q)$ and $\sigma(\bar{y})/\bar{y} = \bar{u}/\bar{v}$. We can then choose $r = \sigma^{-i}(q)\sigma^{-i+1}(q)\cdots\sigma^{-1}(q)$ as a polynomial, so y and $\bar{y}$ will be similar. Likewise, if $\sigma^{r-1}(v)$ and $\sigma^i(u)$ share a nontrivial common factor q, then we can write $u = \sigma^{-i}(q)\bar{u}$ and $v = \sigma^{-r+1}(q)\bar{v}$ for some polynomials $\bar{u}, \bar{v}$. In this case, any hypergeometric term y with $\sigma(y)/y = u/v$ can be viewed as a product $y = r\bar{y}$ of two hypergeometric terms $r, \bar{y}$ with $\sigma(r)/r = \sigma^{-i}(q)/q$ and $\sigma(\bar{y})/\bar{y} = \bar{u}/\bar{v}$. We can then choose $r = 1/(q\sigma^{-1}(q)\cdots\sigma^{-i+1}(q))$ as a rational function, so y and $\bar{y}$ will again be similar.

Thus, the key observation is that if y is a hypergeometric solution of the recurrence, then we can write $y = r\bar{y}$ for some rational function r and a hypergeometric term $\bar{y}$ with $\sigma(\bar{y})/\bar{y} = \bar{u}/\bar{v}$ for some polynomials $\bar{u}, \bar{v}$ with $\bar{u} \mid p_0$ and $\sigma^{r-1}(\bar{v}) \mid p_r$. In some sense, we split the hypothetical solution y into a rational part r and a non-rational part $\bar{y}$ in such a way that the non-rational part is as small as possible. The next definition makes this idea precise.

Definition 2.72 (See Definition 3.70 for the differential case) Let y be a hypergeometric term and let $u, v \in C[x]$ be such that $\sigma(y)/y = u/v$.

1. y is called a *kernel* if $\gcd(u, \sigma^i(v)) = 1$ for all $i \in \mathbb{Z}$.
2. $r \in C(x)$ is called a *shell* for y if the hypergeometric term y/r is a kernel. □

Example 2.73

1. For $y = x\,x!$ we have $\sigma(y)/y = (x+1)^2/x$. In this case, we can take $r = x$ as a shell, because $y/x = x!$ is a kernel.
2. For $y = x!/(x-1)$ we have $\sigma(y)/y = x(x+1)/(x-2)$. In this case, we can take $r = 1/(x-1)$ as a shell, because $y/r = x!$ is a kernel. Alternatively, we can take $r = x$, because for this choice we have $y/x = (x-2)!$, which is also a kernel. □

As we have seen in the example above, it is possible that a hypergeometric term admits more than one decomposition into a shell and a kernel. According to the following lemma, there is always at least one such decomposition.

Lemma 2.74 *Every hypergeometric term can be written as the product of a shell and a kernel.*

Proof Let y be a hypergeometric term, and let $u, v \in C[x]$ be such that $\sigma(y)/y = u/v$. If y is a kernel, we can write $y = 1y$ with 1 as shell, and we are done. If y is not a kernel, there exists an $i \in \mathbb{Z}$ with $\gcd(u, \sigma^i(v)) \neq 1$. Fix such an i, let $q = \gcd(u, \sigma^i(v))$, and let r be a rational function with $\sigma(r)/r = q/\sigma^{-i}(q)$. Such a rational function exists: depending on whether i is positive or negative, we can take $r = \sigma^{-i}(q)\cdots\sigma^{-1}(q)$ or $r = 1/(q\cdots\sigma^{-i+1}(q))$. For the hypergeometric term $\bar{y} = y/r$ we have $\sigma(\bar{y})/\bar{y} = \bar{u}/\bar{v}$ with $\bar{u} = u/q$ and $\bar{v} = v/\sigma^{-i}(q)$. If $\bar{y}$ is a kernel, we have found the desired decomposition $y = r\bar{y}$. If not, apply the same argument to $\bar{y}$. Because of $\deg(\bar{u}) < \deg(u)$ and $\deg(\bar{v}) < \deg(v)$, the argument can only be repeated finitely many times. When it cannot be applied any more, we must have reached a kernel. ■

The proof of the lemma can be translated into an algorithm for computing a decomposition of a given hypergeometric term into a shell and a kernel. For our purpose it is not necessary to compute such a decomposition. Instead, we use its existence for justifying the following algorithm, which proceeds by first finding potential kernels of hypergeometric solutions and then finding for every candidate the corresponding shells using one of the algorithms discussed in the previous section.

Algorithm 2.75
Input: $p_0, \ldots, p_r \in C[x]$ *with* $p_0, p_r \neq 0$.
Output: *A set S of hypergeometric terms y with* $p_0 y + \cdots + p_r\sigma^r(y) = 0$ *such that every other hypergeometric solution of this recurrence is a C-linear combination of elements of S.*

1 *Let* $S = \emptyset$.
2 *for all monic divisors* u *of* p_0 *do*
3 *for all monic divisors* v *of* $\sigma^{-r+1}(p_r)$, *do*
4 *Set* $\bar{p}_i = p_i u \cdots \sigma^{i-1}(u)\sigma^i(v) \cdots \sigma^{r-1}(v)$ *for* $i = 0, \dots, r$ *and let* χ *be the characteristic polynomial of the equation* $\bar{p}_0 y + \cdots + \bar{p}_r \sigma^r(y) = 0$.
5 *for all nonzero roots* $\phi \in C$ *of* χ *do*
6 *Find a basis* B *of the space of all* $q \in C(x)$ *with* $\bar{p}_0 q + \bar{p}_1 \phi \sigma(q) + \cdots + \bar{p}_r \phi^r \sigma^r(q) = 0$.
7 *for each* $q \in B$ *do*
8 *Add to* S *a hypergeometric term* y *with* $\frac{\sigma(y)}{y} = \frac{\phi\sigma(q)u}{qv}$.
9 *Return* S.

Note that the formulation of the output specification takes into account that the set of hypergeometric solutions does not form a vector space in general. The set of hypergeometric solutions (together with zero) is rather a union of vector spaces, each of which consists of hypergeometric terms that are similar to each other.

Note also that u and v need to loop not only over the irreducible factors but over all divisors, including the trivial divisors 1 and p_0 or p_r, respectively.

Theorem 2.76 *Algorithm 2.75 is correct.* □

Proof Let V be the C-vector space generated by the output set of the algorithm, and let W be the C-vector space generated by all hypergeometric solutions of the recurrence. We need to show that $V = W$.

"$\subseteq$": If y is in the output set, say $\frac{\sigma(y)}{y} = \frac{\phi\sigma(q)u}{qv}$, then, by the definition of the $\bar{p}_i$ and the choice of q, we have

$$\begin{aligned} p_0 y + \cdots + p_r \sigma^r(y) &= \Big(p_0 + p_1 \phi \frac{\sigma(q)}{q}\frac{u}{v} + \cdots + p_r \phi^r \frac{\sigma^r(q)}{q}\frac{u \cdots \sigma^{r-1}(u)}{v \cdots \sigma^{r-1}(v)}\Big) y \\ &= \frac{\bar{p}_0 q + \bar{p}_1 \phi \sigma(q) + \cdots + \bar{p}_r \phi^r \sigma^r(q)}{q\, v \cdots \sigma^{r-1}(v)} y = 0. \end{aligned}$$

"$\supseteq$": We need to show that if y is a hypergeometric solution of the recurrence, then it can be written as a C-linear combination of the elements of the output set. Consider an arbitrary hypergeometric solution y. According to Lemma 2.74, we can write $y = q\bar{y}$ where $\bar{y}$ is a kernel and q is a shell. Fix such a decomposition and let $\psi \in C$ and $u, v \in C[x] \setminus \{0\}$ be monic and such that $\frac{\sigma(\bar{y})}{\bar{y}} = \psi \frac{u}{v}$. By Definition 2.72, we then have $\gcd(u, \sigma^i(v)) = 1$ for all $i \in \mathbb{Z}$. Therefore, according to the discussion right before Definition 2.72, we have $u \mid p_0$ and $v \mid p_r$. In the iteration where the algorithm checks the pair (u, v), we have $\bar{p}_0 q + \bar{p}_1 \psi \sigma(q) + \cdots + \bar{p}_r \psi^r \sigma^r(q) = 0$. As shown in Exercise 11 of Sect. 2.5, a linear recurrence can only have rational solutions if 1 is a root of its characteristic polynomial. Therefore, ψ must be one of the ϕ's considered in the loop starting at line 5. But then, q must be a linear combination of the elements of the set B computed in line 6, and therefore y must be a linear combination of the hypergeometric terms formed in line 7. It is therefore in particular a linear combination of elements of the output set, as claimed. ■

Example 2.77

1. Consider the recurrence

$$55(2x+5)y - (47x+149)\sigma(y) + 5(x+4)\sigma^2(y) = 0.$$

Following Algorithm 2.75, we have to inspect all pairs (u, v) of monic polynomials such that $u \mid (2x+5)$ and $\sigma^1(v) \mid (x+4)$. There are four such pairs: $(1, 1)$, $(1, x+3)$, $(x+\frac{5}{2}, 1)$, $(x+\frac{5}{2}, x+3)$. Three of these do not lead to solutions. For the remaining pair $(x+\frac{5}{2}, x+3)$, we get in line 4 the modified recurrence

$$\begin{aligned}55(2x+5)(x+3)(x+4)y &- (47x+149)(x+\tfrac{5}{2})(x+4)\sigma(y)\\ &+ 5(x+4)(x+\tfrac{5}{2})(x+\tfrac{7}{2})\sigma^2(y) = 0,\end{aligned}$$

which after clearing the common factor $(x+\frac{5}{2})(x+4)$ simplifies to

$$110(x+3)y - (47x+149)\sigma(y) + 5(x+\tfrac{7}{2})\sigma^2(y) = 0.$$

The characteristic polynomial $\chi = 110 - 47x + 5x^2 = (x-5)(5x-22)$ has the two roots 5 and 22/5. For the root $\phi = 5$, we consider the modified equation

$$110(x+3)y - 5(47x+149)\sigma(y) + 125(x+\tfrac{7}{2})\sigma^2(y) = 0,$$

which has no solution in $C(x)$. For the root $\phi = 22/5$, we consider the modified equation

$$110(x+3)y - \tfrac{22}{5}(47x+149)\sigma(y) + \tfrac{484}{5}(x+\tfrac{7}{2})\sigma^2(y) = 0.$$

Its solution space in $C(x)$ is generated by $\{3x-5\}$.
It follows that the only hypergeometric solutions of the original equation are the hypergeometric terms y with $\frac{\sigma(y)}{y} = \frac{11(2x+5)(3x-2)}{5(x+3)(3x-5)}$.

2. In general, the existence of hypergeometric solutions depends on the constant field. For example, the recurrence

$$\begin{aligned}(x^2+2x-4)f(x) &- (2x+3)(x^2+2x-4)f(x+1)\\ &+(x^2+2x-4)(x^2+4x-1)f(x+2) = 0\end{aligned}$$

has no hypergeometric solutions over $\mathbb{Q}(x)$, but it does have hypergeometric solutions over $\bar{\mathbb{Q}}(x)$, namely the terms y with $\sigma(y)/y = 1/(x+\sqrt{5}+1)$ or $\sigma(y)/y = 1/(x-\sqrt{5}+1)$. □

It can be shown (Exercise 8) that Algorithm 2.75 remains correct when in line 6 we only search for polynomial solutions. This variant is known as Petkovšek's algorithm. Finding all polynomial solutions of an equation is obviously cheaper than finding all of its rational solutions, and it is a good idea to save time in this step because we have to solve a lot of equations: the number of pairs (u, v) considered by the algorithm is exponential in the degree of $p_0 p_r$. In order to further improve the performance of the algorithm, it is worthwhile to make an effort at reducing the number of pairs it has to consider. Here are three ideas for doing so.

1. In the proof of Theorem 2.76, we have seen that it suffices to consider pairs (u, v) which form the kernel of a hypergeometric solution. We can therefore safely discard all pairs (u, v) with $\gcd(u, \sigma^i(v)) \neq 1$ for some $i \in \mathbb{Z}$. In Petkovšek's algorithm, where we only search for polynomial solutions in line 6, we can only discard those pairs (u, v) with $\gcd(u, \sigma^i(v)) \neq 1$ for some $i \in \mathbb{N}$.
2. When we consider a certain divisor u of p_0 in line 2, we do not also need to consider any other divisor of the form $\sigma^i(u)$ of p_0, for any $i \in \mathbb{Z}\setminus\{0\}$. The reason is that considering $\sigma^i(u)$ would only produce hypergeometric solutions which are C-linear combinations of those already found (Exercise 9). The analogous reasoning applies to the divisors v of p_r. In Petkovšek's algorithm, where we only search for polynomial solutions in line 6, we must choose the divisors u of p_0 which are left-most in the sense that $\sigma^i(u) \nmid p_0$ for all $i < 0$, and the divisors v of $\sigma^{-r}(p_r)$ which are right-most in the sense that $\sigma^i(v) \nmid \sigma^{-r}(p_r)$ for all $i > 0$.
3. Hypergeometric terms correspond to generalized series solutions of a very special form (see Exercise 14 of Sect. 2.4). Using the algorithm described in Sect. 2.4, we can compute all $e \in \mathbb{Z}$, $\rho \in \bar{C}$ and $\alpha \in \bar{C}$ such that there is a generalized series solution of the form $\Gamma(x)^e \rho^x x^\alpha (1 + \cdots)$. Since we do not need to worry about subexponential parts or logarithmic terms, this data is easy to compute. A pair (u, v) can only give rise to a hypergeometric solution if the degree difference $\deg_x(u) - \deg_x(v)$ matches one of the exponents e appearing in the generalized series solutions. Furthermore, rather than all roots of the characteristic polynomial, we only need to test the values ρ appearing in the generalized series solutions with $e = \deg_x(u) - \deg_x(v)$.

Each of these filters cuts down the number of pairs considerably, and an implementation of Algorithm 2.75 should definitely take advantage of all three of them. Let us have a closer look at the third filter. We are exploiting here that the existence of hypergeometric solutions corresponds to the existence of some other kind of solutions, about which we can easily obtain at least partial information. As a consequence of the following lemma, this works more generally.

Lemma 2.78 *(See Lemma 3.73 for the differential case) Consider a recurrence operator $L = p_0(x) + p_1(x)S + \cdots + p_r(x)S^r \in C(x)[S]$. Then L has a hypergeometric solution y with $\sigma(y)/y = u/v$ if and only if L has a first order right factor $u - vS$.*

Proof "$\Rightarrow$": Define $q_{r-1} = p_r/\sigma^{r-1}(v)$ and recursively $q_i = (q_{i+1}\sigma^{i+1}(u) + p_{i+1})/\sigma^i(v)$ for $i = r-2, \ldots, 0$. Then it can be checked by a calculation that

$$p_r S^r + \cdots + p_0 = (q_{r-1} S^{r-1} + \cdots + q_0)(vS - u) + t,$$

where $t = p_0 + \frac{u}{v} p_1 + \cdots + \frac{u\sigma(u)\cdots\sigma^{r-1}(u)}{v\sigma(v)\cdots\sigma^{r-1}(v)} p_r \in C(x)$.

If y is a hypergeometric term with $\sigma(y)/y = u/v$, then it can also be checked by a calculation that $L \cdot y = ty$.

Therefore, if y is a solution of L, we have $L \cdot y = ty = 0$, so $t = 0$, and so $vS - u$ is a right factor of L.

"$\Leftarrow$": Clearly y is a solution of $u - vS$. If $L = Q(u - vS)$ for some operator $Q \in C(x)[S]$, then $L \cdot y = Q(u - vS) \cdot y = Q \cdot \big((u - vS) \cdot y\big) = Q \cdot 0 = 0$, so y is a solution of L. ■

Using this lemma, it is easy to justify the correctness of the third filter: if the recurrence at hand has a hypergeometric solution, then the corresponding operator has a first order right hand factor, and then this right hand factor has a generalized series solution of the form described in Exercise 14 of Sect. 2.4, and since this series is a solution of a right factor it is also a solution of the whole operator.

The basic idea of the next algorithm is to apply this reasoning to sequence solutions of deformed recurrences instead of generalized series. For simplicity, let us assume that C is algebraically closed. For every fixed $\alpha + \mathbb{Z} \in C/\mathbb{Z}$, consider the space of all the sequence solutions $a \colon \alpha + \mathbb{Z} \to C((q))$ of the deformed recurrence. Suppose the undeformed recurrence has a hypergeometric solution y with $\sigma(y)/y = u/v$. Then, since the operator corresponding to this recurrence must have $u - vS$ as right factor, the deformed recurrence contains $u(x+q) - v(x+q)S$ as right factor, and hence the space of sequence solutions of the deformed recurrence must contain a sequence a with $u(n+q)a(n) - v(n+q)a(n+1) = 0$ for all $n \in \mathbb{Z}$.

The singularity pattern of a is determined by the factors of u and v which are shift equivalent to $x - \alpha$. Write $\nu(n)$ for the smallest exponent of q appearing in $a(n) \in C((q))$. By replacing a by $q^k a$ for suitable $k \in \mathbb{Z}$, we can ensure that $\nu(n) = 0$ for all $n \in \mathbb{Z}$ below a certain $n_{\min} \in \mathbb{Z}$. Starting from any such sufficiently small index n, the deformed recurrence uniquely determines all the subsequent terms. In particular, we have $\nu(n+1) = \nu(n) + k$ if $k \in \mathbb{N}$ is the multiplicity of $x - n - \alpha$ in u, and $\nu(n+1) = \nu(n) - k$ if $k \in \mathbb{N}$ is the multiplicity of $x - n - \alpha$ in v. (As before, we may assume that u and v are coprime.) Eventually, for all n above a certain threshold $n_{\max} \in \mathbb{Z}$, we will have $\nu(n) = \nu(n+1) = \cdots$. The number $m \in \mathbb{Z}$ with $m = \nu(n)$ for all sufficiently large $n \in \mathbb{Z}$ is called the *valuation growth* of a. The valuation growth of a at some $\alpha + \mathbb{Z} \in C/\mathbb{Z}$ is uniquely determined by u and v. For solutions of higher order equations, it is a bit more tricky to define the valuation growth properly. For example, the recurrence $f(n+2) - f(n) = 0$ has the periodic solution $\ldots, 1, q, 1, q, 1, q, \ldots$ for which the valuation does not stabilize for sufficiently large or sufficiently small index. It remains true, however, that for all sufficiently small and all sufficiently large indices n, the valuation of a sequence term $a(n)$ is at least as much as $\min_{i=1}^{r} \nu(a(n+i))$ and at least as much as $\min_{i=1}^{r} \nu(a(n-i))$. This has the following consequence, on which a valid definition of the valuation growth can be based.

Lemma 2.79 *Let* $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$, *and* $\alpha + \mathbb{Z} \in C/\mathbb{Z}$. *Let* $a\colon \alpha + \mathbb{Z} \to C((q)) \setminus \{0\}$ *be such that*

$$p_0(n+q)a(n) + \cdots + p_r(n+q)a(n+r) = 0$$

for all $n \in \alpha + \mathbb{Z}$. *Then* $\liminf_{n\to\infty} \nu(a(\alpha+n))$ *and* $\liminf_{n\to\infty} \nu(a(\alpha-n))$ *exist.*

Proof If $\liminf_{n\to\infty} \nu(a(\alpha+n))$ does not exist, then there are infinitely many indices $n_0 \in \mathbb{N}$ such that $\nu(a(\alpha+n_0)) < \nu(a(\alpha+n))$ for all $n > n_0$. This is impossible, because if n_0 is such that $\alpha + n_0$ is not a root of p_0, then $a(\alpha+n_0)$ is a $C[[q]]$-linear combination of $a(\alpha+n_0+i)$ for $i = 1, \ldots, r$, and therefore $\nu(a(\alpha+n_0)) \geq \min_{i=1}^r \nu(a(\alpha+n_0+i))$. This shows that $\liminf_{n\to\infty} \nu(a(\alpha+n))$ exists. The existence of $\liminf_{n\to\infty} \nu(a(\alpha-n))$ is shown by an analogous argument. ■

Definition 2.80 Let $p_0, \ldots, p_r \in C[x]$, not all zero, and $\alpha + \mathbb{Z} \in C/\mathbb{Z}$. Let $a\colon \alpha + \mathbb{Z} \to C((q)) \setminus \{0\}$ be such that

$$p_0(n+q)a(n) + \cdots + p_r(n+q)a(n+r) = 0$$

for all $n \in \alpha + \mathbb{Z}$. Then the number

$$\liminf_{n\to\infty} \nu(a(\alpha+n)) - \liminf_{n\to\infty} \nu(a(\alpha-n)) \in \mathbb{Z}$$

is called the *valuation growth* of a at $\alpha + \mathbb{Z}$. □

Example 2.81

1. The valuation growth of a hypergeometric term is easy to determine. If y is such that $\sigma(y)/y = u/v$ for some polynomials $u, v \in C[x]$, then the valuation growth of y at $\alpha + \mathbb{Z}$ is equal to $A - B$, where A is the number of roots of u in $\alpha + \mathbb{Z}$ and B is the number of roots of v in $\alpha + \mathbb{Z}$.
   For example, the term $x!$ has valuation growth 1 at $\mathbb{Z}$, the term $(2x)!/x!^3$ has valuation growth -1 at $\mathbb{Z}$, the term $x!^9(x-1/2)!^2$ has valuation growth 2 at $\frac{1}{2} + \mathbb{Z}$, and so on.
2. Consider the sequence $a\colon \mathbb{Z} \to \mathbb{Q}((q)) \setminus \{0\}$ defined by $a(0) = 1$, $a(1) = 0$, and $a(n) = a(n-2)$ for $n \in \mathbb{Z}$. For this sequence we have $\liminf_{n\to\infty} \nu(a(n)) = 0$ and $\liminf_{n\to\infty} \nu(a(-n)) = 0$, so its valuation growth is zero.
3. The sequence $a\colon \mathbb{Z} \to \mathbb{Q}((q)) \setminus \{0\}$ defined by $a(n) = q^{n^2}$ cannot be the solution of a deformed D-finite recurrence equation, and no valuation growth is associated to it. □

The valuation growth of a solution of a recurrence $p_0 f + \cdots + p_r \sigma^r(f) = 0$ can be modulated by applying suitable substitutions to the recurrence. If f has valuation growth m at α and h is a hypergeometric term such that $\sigma(h)/h = (x-\alpha)^m$, plug $f = hg$ for a new unknown g into the equation, and divide by h to obtain a recurrence with rational function coefficients for g. A hypergeometric term y is a solution of the original recurrence if and only if y/h is a hypergeometric solution of the new recurrence. This means that the substitution turns any sequence solution a of the deformed original recurrence into a sequence solution with valuation growth zero of the deformed new recurrence.

A fixed recurrence can only have solutions with nonzero valuation growth for finitely many classes $\alpha + \mathbb{Z}$, because any class for which the valuation growth is nonzero must contain at least a root of p_r or a root of p_0, and these are just finitely many. It follows in particular that for every hypergeometric term y there exist $\alpha_1, \ldots, \alpha_k \in C$ and $m_1, \ldots, m_k \in \mathbb{Z}$ such that the hypergeometric term y/h has valuation growth zero for all classes $\alpha + \mathbb{Z}$, when h is chosen as the hypergeometric term defined by $\sigma(h)/h = (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}$. Now by Exercise 15 the only hypergeometric terms which have valuation growth zero for all $\alpha + \mathbb{Z}$ have the form $r(x)\phi^x$ with a rational function r and a constant $\phi \in C$. We already know how to find such solutions.

In order to find the hypergeometric solutions of a recurrence $p_0 f + \cdots + p_r\sigma^r(f) = 0$, it would therefore be sufficient if for every $\alpha + \mathbb{Z}$ we could determine finite lower and upper bounds on the possible valuation growth of these hypergeometric solutions. Then we can go through all combinations of the growth candidates at the various classes $\alpha + \mathbb{Z}$ and for each of them apply a substitution to the equation and see whether the transformed equation has solutions of the form $r(x)\phi^x$. This algorithm will still suffer from combinatorial explosion, but the number of combinations it has to consider is considerably smaller than for Algorithm 2.75.

Before we formulate the algorithm in detail, let us discuss how to find bounds for the valuation growth. First observe that the valuation can drop only at indices where the leading coefficient of the recurrence has a root and can raise only where the trailing coefficient of the recurrence has a root. As a naive choice, we could therefore simply take $-\deg_x p_r$ as lower bound and $\deg_x p_0$ as upper bound. A better bound can be obtained by ignoring irrelevant factors of p_0 and p_r. For a fixed $\alpha + \mathbb{Z} \in C/\mathbb{Z}$, the possible valuation growths can only depend on the roots of p_0 and p_r in $\alpha + \mathbb{Z}$, and other factors can be ignored. We can therefore take as a lower bound $-\sum_{n\in\mathbb{Z}} \nu_{\alpha+n}(p_r)$ and as an upper bound $\sum_{n\in\mathbb{Z}} \nu_{\alpha+n}(p_0)$, where $\nu_\xi(p)$ denotes the multiplicity of the root ξ in the polynomial p.

It is possible to refine the bounds further. In order to get a lower bound, consider a basis $\{b_1, \ldots, b_r\}$ of the space of solutions $a\colon \alpha + \mathbb{Z} \to C((q))$. We can choose initial values $b_i(\alpha + n_{\min} - j) = \delta_{i,j}$ for $i, j = 1, \ldots, r$, for some fixed $n_{\min} \in \mathbb{Z}$ which is such that $p_0(\alpha + n)p_r(\alpha + n) \neq 0$ for all $n < n_{\min}$. Then $\liminf_{n\to\infty} \nu(b_i(\alpha - n)) = 0$ for $i = 1, \ldots, r$. Now choose some $n_{\max} \in \mathbb{Z}$ which is such that $p_0(\alpha + n)p_r(\alpha + n) \neq 0$ for all $n > n_{\max}$ and compute $b_i(\alpha + n_{\max} + j)$ for $i, j = 1, \ldots, r$. Then $\liminf_{n\to\infty} \nu(b_i(\alpha + n)) \geq \min_{j=1}^r \nu(b_i(\alpha + n_{\max} + j))$. As any hypergeometric solution must correspond to a certain $C((q))$-linear combination of $b_1, \ldots, b_r$, the valuation growth of such a solution cannot be smaller than $\min_{i,j=1}^r \nu(b_i(\alpha + n_{\max} + j))$, so we can use this number as a lower bound. An upper bound can be determined analogously by imposing initial conditions

$b_i(\alpha + n_{\max} + j) = \delta_{i,j}$ and observing that the valuation growth cannot be smaller than $-\min_{i,j=1}^{r} \nu(b_i(\alpha + n_{\min} - j))$.

Algorithm 2.82 *(van Hoeij; see Algorithm 3.74 for the differential case.)*
Input: *polynomials $p_0, \ldots, p_r \in C[x]$ with $p_0, p_r \neq 0$. It is assumed that C is algebraically closed.*
Output: *A set H of hypergeometric terms y with $p_0 y + \cdots + p_r \sigma^r(y) = 0$ such that every other hypergeometric solution of this recurrence is a C-linear combination of elements of H.*

1 *Determine the set of all triples $(e, \phi, d + \mathbb{Z}) \in \mathbb{Z} \times C \times (C/\mathbb{Z})$ such that the recurrence has a generalized series solution of the form $\Gamma(x)^e \phi^x x^d (1 + \cdots)$.*
2 *Determine a set $\{\alpha_1, \ldots, \alpha_k\} \subseteq C$ with $\alpha_i - \alpha_j \notin \mathbb{Z}$ for $i \neq j$ and such that for every root ξ of $p_0 p_r$ there exist $i \in \{1, \ldots, k\}$ and $n \in \mathbb{Z}$ with $\xi = \alpha_i + n$.*
3 *For every $i = 1, \ldots, k$, determine $m_i^{\min}, m_i^{\max} \in \mathbb{Z}$ such that the valuation growth m of any hypergeometric solution at $\alpha_i + \mathbb{Z}$ satisfies $m_i^{\min} \leq m \leq m_i^{\max}$*
4 *Set $H = \emptyset$.*
5 *for all tuples $(m_1, \ldots, m_k) \in \{m_1^{\min}, \ldots, m_1^{\max}\} \times \cdots \times \{m_k^{\min}, \ldots, m_k^{\max}\}$ do*
6   *for all tuples $(e, \phi, d + \mathbb{Z})$ from line 1 with $e = \sum_{i=1}^k m_i$ and $\sum_{i=1}^k m_i \alpha_i \in d + \mathbb{Z}$ do*
7   *Apply a change of variables $y = \bigl(\prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i}\bigr)\phi^x \tilde{y}$ to the input recurrence and find a basis $\{b_1, \ldots, b_\ell\} \subseteq C(x)$ of the space of all rational solutions $\tilde{y}$ of the resulting recurrence.*
8   *Let $H = H \cup \bigl\{\bigl(\prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i}\bigr)\phi^x b_j : j = 1, \ldots, \ell\bigr\}$.*
9 *Return H.*

Theorem 2.83 *Algorithm 2.82 is correct.* □

Proof It is clear by construction that every element of the output set is a hypergeometric solution of the input recurrence. Conversely, suppose that y is any hypergeometric solution of the input recurrence. We have to show that it is a C-linear combination of elements of the output set H. Let $\alpha + \mathbb{Z} \in C/\mathbb{Z}$. If $p_0 p_r$ has no root in $\alpha + \mathbb{Z}$, then the valuation growth of every solution of the recurrence at $\alpha + \mathbb{Z}$ is zero, in particular the valuation growth of y. Therefore, the valuation growth of y can be nontrivial only for the classes $\alpha_i + \mathbb{Z}$ considered by the algorithm. For every $i \in \{1, \ldots, k\}$, the valuation growth of y at $\alpha_i + \mathbb{Z}$ must be in the range $m_i^{\min}, \ldots, m_i^{\max}$. Therefore, the loop in line 5 will go through one iteration where $(m_1, \ldots, m_k)$ is the vector of valuation growths of y. Then $y / \prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i}$ has the form $\phi^x \tilde{y}(x)$ for some $\phi \in C$ and some rational function $\tilde{y} \in C(x)$ (Exercise 15). Since $\prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i} \phi^x \tilde{y}(x)$ corresponds to a generalized series solution of the form $\Gamma(x)^{m_1 + \cdots + m_k} \phi^x x^{m_1\alpha_1 + \cdots + m_k\alpha_k + \ell}(1 + \cdots)$, where $\ell \in \mathbb{Z}$ is the degree difference of numerator and denominator of $\tilde{y}(x)$, the only candidates for ϕ are those which are selected in the loop of line 6. For one of these ϕ, we have that $y/((\prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i})\phi^x)$ is a rational function, which can then only be a C-linear combination of the basis elements $b_1, \ldots, b_r$ computed in line 7 of the corresponding iteration. Then y itself is a C-linear combination of the hypergeometric terms added to H in line 8, and hence also a C-linear combination of the output set. ■

Example 2.84 Consider again the recurrence

$$55(2x+5)y - (47x+149)\sigma(y) + 5(x+4)\sigma^2(y) = 0$$

from Example 2.77. This recurrence has the two generalized series solutions $\Gamma(x)^0(\frac{22}{5})^x x^{1/2}(1+\cdots)$ and $\Gamma(x)^0 5^x x^{-2}(1+\cdots)$, from which we get the triples $(0, \frac{22}{5}, \frac{1}{2}+\mathbb{Z})$ and $(0, 5, \mathbb{Z})$.

In line 2, we can take $\alpha_1 = 1/2$ to cover the root of $2x+5$ and $\alpha_2 = 0$ to cover the root of $x+4$. In the equivalence class $\mathbb{Z}$, a solution may or may not experience a drop by one when passing through the point $n = 2$, because of the factor $x+4$. Therefore, we can take $m_2^{\min} = -1$ and $m_2^{\max} = 0$. Going in the opposite direction through the equivalence class $\frac{1}{2}+\mathbb{Z}$, we observe the same behavior, which implies for the right direction that there may or may not be an increase by one when passing through the point $n = 2$. Therefore, we can take $m_1^{\min} = 0$, $m_2^{\max} = 1$.

In the loop of line 5, there are four pairs (m_1, m_2) to be considered: $(0,-1)$, $(0,0)$, $(1,0)$, $(1,-1)$. In line 6, only the pair $(1,-1)$ passes the filter, and the only matching triple is $(0, \frac{22}{5}, \frac{1}{2}+\mathbb{Z})$. In line 7 we plug $y = \frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)}(\frac{22}{5})^x\tilde{y}$ into the input recurrence and divide by $\frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)}(\frac{22}{5})^x$ to obtain

$$55(2x+5)\tilde{y} - \frac{11(47x+149)(2x+1)}{5x}\sigma(\tilde{y}) + \frac{121(2x+3)(2x+1)(x+4)}{5x(x+1)}\sigma^2(\tilde{y}) = 0.$$

The solution space of this recurrence in $C(x)$ is generated by $\{\frac{(2x+1)(2x+3)(3x-5)}{5x(x+1)(x+2)}\}$.

It follows that the hypergeometric solutions of the input recurrence are precisely the nonzero constant multiples of $\frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)}(\frac{22}{5})^x\frac{(2x+1)(2x+3)(3x-5)}{5x(x+1)(x+2)}$. This result is consistent with the result obtained in Example 2.77. □

The main bottleneck of Algorithm 2.82 is the number of iterations of the loop starting in line 5. Although the number of combinations $(m_1, \ldots, m_k)$ which have to be considered is typically much smaller than the number of combinations inspected by Algorithm 2.75, we are still in danger of facing a combinatorial explosion. In examples, almost none of the tuples survives the filter of line 6.

A careful implementation of Algorithm 2.82 should also take into account the following improvements.

1. Let $e_1, \ldots, e_\ell \in \mathbb{Z}$ be the first components of the tuples found in line 1. It is quite likely that some of the ranges $\{m_i^{\min}, \ldots, m_i^{\max}\}$ contain more than ℓ integers. Suppose for example that $i = 1$ has the longest range and that it has more than ℓ elements. Then instead of checking for each tuple $(m_1, \ldots, m_k) \in \{m_1^{\min}, \ldots, m_1^{\max}\} \times \cdots \times \{m_k^{\min}, \ldots, m_k^{\max}\}$ whether $\sum_{i=1}^k m_i \in \{e_1, \ldots, e_\ell\}$, it is better to check for each tuple

$$(e, m_2, \dots, m_k) \in \{e_1, \dots, e_\ell\} \times \{m_2^{\min}, \dots, m_2^{\max}\} \times \cdots \times \{m_k^{\min}, \dots, m_k^{\max}\}$$

whether $e - \sum_{i=2}^k m_i \in \{m_1^{\min}, \dots, m_1^{\max}\}$.

2. Once we have found a hypergeometric solution, we can take this information into account in the subsequent search. For every tuple $(e, \phi, d + \mathbb{Z})$ found in line 1, we can also determine the dimension of the C-vector space generated by all generalized sequence solutions of the form $\Gamma(x)^e \phi^x x^d (x^n + \cdots)$ and record this number together with the tuple. Whenever we find a bunch of ℓ solutions in line 7, we reduce the dimension associated to the corresponding tuple $(e, \phi, d + \mathbb{Z})$ by ℓ. Then in line 6 we only need to take into account tuples $(e, \phi, d + \mathbb{Z})$ for which the associated dimension is still positive.
3. The α_i chosen in line 2 are representatives of the equivalence classes $\alpha_i + \mathbb{Z}$. The choice of the representatives does not matter for the correctness of the algorithm but it may influence its performance. If, for example, we select $\alpha = 100$ and one of the solutions is $\Gamma(x)$, then the rational functions constructed in line 7 will contain the large compensating factor $\Gamma(x)/\Gamma(x+100) = \frac{1}{x(x+1)\cdots(x+99)}$, which would not show up if we choose $\alpha = 0$.
   The optimal choice of representatives will not be known until we have found all hypergeometric solutions, but we can at least try to make a reasonable choice in line 2. One option that seems to be reasonable is to choose every α_i somewhere in the middle between the smallest root of p_0 in $\alpha_i + \mathbb{Z}$ and the largest root of p_r in $\alpha_i + \mathbb{Z}$.
4. When the bounds on the valuation growth in line 3 are determined using bases of sequence solutions of the deformed equation, then this computation should be done in a finite field rather than in C. When α_i is irrational with minimal polynomial $u \in \mathbb{Z}[x]$, we choose a prime p such that u has a linear factor when viewed as an element of $\mathbb{Z}_p[x]$. Such primes can be found by trial and error. Then α_i can be mapped to the root of u in $\mathbb{Z}_p$.
5. It is possible to avoid the computation of denominator bounds in line 7. Instead of computing them there, we compute the possible contribution to a denominator bound for each α_i while we determine the bounds $m_i^{\min}$ and $m_i^{\max}$ in line 3 by inspecting the valuations of the series solutions of the deformed equation, like for Algorithm 2.67. If we include this denominator bound in the change of variables of line 7, it suffices to solve for polynomial solutions.
   We can also get a degree bound for the polynomial solutions almost for free. If $v \in C[x]$ is a denominator bound and we apply the change of variables $y = \frac{1}{v}(\prod_{i=1}^k \Gamma(x + \alpha_i)^{m_i})\phi^x \tilde{y}$ for an unknown polynomial $\tilde{y}$, the corresponding generalized series solution has the form $\Gamma(x)^{m_1+\cdots+m_k} \phi^x x^{m_1\alpha_1+\cdots+m_k\alpha_k+\deg_x \tilde{y}-\deg_x v}(1 + \cdots)$. Therefore, the possible candidates for $\deg_x \tilde{y}$ can be obtained from the exponents of the polynomial parts of the generalized series solutions.

Most recurrence equations do not have any hypergeometric solutions. Most recurrence equations which do have hypergeometric solutions have only one such solution (up to constant multiples of course). If a recurrence has a hypergeometric solution, what can be said about its other solutions?

According to Lemma 2.78, a hypergeometric solution corresponds to a first order right factor of the operator corresponding to the recurrence. If P is the operator corresponding to the recurrence and we have $P = P_1(v_1 S - u_1)$ for some operator P_1 and nonzero polynomials $u_1, v_1 \in C[x]$, then a solution of P_1 can be translated into a solution of P. To be specific, let us consider sequence solutions, and to make this meaningful, let us assume that u_1 and v_1 have no integer roots. Then P has a hypergeometric solution $a_1 \colon \mathbb{N} \to C$ which can be written as $a_1(n) = \prod_{k=0}^{n-1} \frac{u_1(k)}{v_1(k)}$. Let $b_1 \colon \mathbb{N} \to C$ be a solution of P_1. An additional solution $a_2 \colon \mathbb{N} \to C$ of P can be obtained from b_1 by solving the recurrence

$$b_1(n) = v_1(n)a_2(n+1) - u_1(n)a_2(n),$$

because for such a sequence a_2, we have $P \cdot a_2 = P_1(v_1 S - u_1) \cdot a_2 = P_1 \cdot ((v_1 S - u_1) \cdot a_2) = P_1 \cdot b_1 = 0$. It is not hard to solve the inhomogeneous first order equation for a_2 explicitly in terms of b_1, u_1, v_1. To do so, set $a_2(n) = s(n)a_1(n)$, where a_1 is the hypergeometric solution of P and s is a new unknown sequence. Applying the substitution to the equation and dividing by $u_1(n)a_1(n)$ gives

$$s(n+1) - s(n) = \frac{b_1(n)}{u_1(n)a_1(n)}.$$

This is a telescoping equation. Replacing n by k and summing the equation for $k = 0, \ldots, n-1$ yields $s(n) = s(0) + \sum_{k=0}^{n-1} \frac{b_1(k)}{u_1(k)a_1(k)}$, where we may regard $s(0)$ as an arbitrary constant. Taking $s(0) = 0$, we obtain $a_2(n) = a_1(n) \sum_{k=0}^{n-1} \frac{b_1(k)}{u_1(k)a_1(k)}$ as an additional solution of P.

If the solution b_1 of P_1 is hypergeometric, we can iterate the construction. In this case, we have $P_1 = P_2(v_2 S - u_2)$ for some operator P_2 and some nonzero polynomials u_2, v_2. Let us assume again for simplicity that u_2 and v_2 have no integer roots. Then $b_1(n) = \prod_{k=0}^{n-1} \frac{u_2(k)}{v_2(k)}$ (up to a constant multiple). A solution $c_1 \colon \mathbb{N} \to C$ of P_2 gives rise to a new solution $b_2(n) = b_1(n) \sum_{k=0}^{n-1} \frac{c_1(k)}{u_2(k)b_1(k)}$ of P_1, which in turn gives rise to a new solution

$$a_3(n) = a_1(n) \sum_{k=0}^{n-1} \frac{b_2(k)}{u_1(k)a_1(k)} = a_1(n) \sum_{k=0}^{n-1} \frac{b_1(k)}{u_1(k)a_1(k)} \sum_{i=0}^{k-1} \frac{c_1(i)}{u_2(i)b_1(i)}$$

of P. In the general case, when we have an operator P of the form $P = \cdots (v_2 S - u_2)(v_1 S - u_1)$ for some nonzero polynomials $v_1, u_1, v_2, u_2, \ldots$, define $h_i(n) = \prod_{k=0}^{n-1} \frac{u_i(k)}{v_i(k)}$ for $i = 1, 2, \ldots$, so that $(v_i S - u_i) \cdot h_i = 0$ for $i = 1, 2, \ldots$. Then these hypergeometric terms translate into the following solutions of P:

$$h_1(n),$$

$$h_1(n)\sum_{k=0}^{n-1}\frac{h_2(k)}{u_1(k)h_1(k)},$$

$$h_1(n)\sum_{k=0}^{n-1}\left(\frac{h_2(k)}{u_1(k)h_1(k)}\sum_{i=0}^{k-1}\frac{h_3(i)}{u_2(i)h_2(i)}\right),$$

$$h_1(n)\sum_{k=0}^{n-1}\left(\frac{h_2(k)}{u_1(k)h_1(k)}\sum_{i=0}^{k-1}\left(\frac{h_3(i)}{u_2(i)h_2(i)}\sum_{j=0}^{i-1}\frac{h_4(j)}{u_3(j)h_3(j)}\right)\right),$$

$$\vdots$$

These solutions are called *d'Alembertian* solutions of P. It is not difficult to show (Exercise 17) that they are linearly independent over C.

Example 2.85 The recurrence

$$(n+2)f(n+2)-(2n+3)f(n+1)+(n+1)f(n)=0$$

has the hypergeometric solution $a_1 = 1$. It corresponds to the operator $S-1$, which must hence be a right factor of the recurrence operator. Indeed, we have the factorization

$$(x+2)S^2-(2x+3)S+(x+1)=((x+2)S-(x+1))(S-1).$$

The left hand factor $P_1 = (x+2)S-(x+1)$ has the rational solution $b_1 = \frac{1}{x+1}$. Consequently, the original recurrence has the second solution $a_2 = 1\sum_{k=0}^{n-1}\frac{1/(k+1)}{1\cdot 1} = \sum_{k=1}^{n}\frac{1}{k}$. Since this sum is obviously not constant and the recurrence has no other hypergeometric solutions, it follows that $H_n = \sum_{k=1}^{n}\frac{1}{k}$ is not hypergeometric. □

Exercises

1. Let y be a hypergeometric term over $C(x)$ and let $y = r\bar{y}$ be such that r is a shell and $\bar{y}$ is a kernel. Show that y is transcendental if and only if $\bar{y}$ is transcendental.

2⋆. Show that all hypergeometric terms over $C(x)$ which are algebraic over $C(x)$ are of the form $r(x)\omega^x$ for some $r(x) \in C(x)$ and some root of unity ω.

3***.** Let y_1, y_2 be hypergeometric over $C(x)$ and suppose that $y_1 + y_2 \neq 0$ and that C is the constant field of $C(x, y_1, y_2)$. Show that $y_1 + y_2$ is hypergeometric if and only if y_1, y_2 are similar.

4. A sequence $a\colon \mathbb{Z} \to C$ is called hypergeometric if it satisfies a first-order linear recurrence with polynomial coefficients. Let a be such a sequence. Show that there exists $n_0 \in \mathbb{Z}$ such that either $a(n) = 0$ for all $n \geq n_0$ or $a(n) \neq 0$ for all $n \geq n_0$.

5. The sequence $a\colon \mathbb{Z} \to C$ is defined by the recurrence

$$4(2n+1)(3n^3+9n^2+5n-3)a(n+2) - 2(21n^4+63n^3+20n^2-59n-27)a(n+1)$$
$$+ (21n^4+60n^3-7n^2-86n-36)a(n+2) - (n+3)(3n^3-4n-2)a(n+3) = 0$$

and the initial values $a(0) = 2$, $a(1) = 3$, $a(2) = 7$. The recurrence has the hypergeometric solutions $\binom{2n}{n}$, 2^n, and n. Express the sequence a as a linear combination of these terms.

6****.** Design an algorithm which for a given hypergeometric term computes a decomposition into kernel and shell.

7****.** (Bill Gosper, Marko Petkovšek) Show that for every $r \in C(x)$ there exist $\phi \in C$ and monic polynomials $a, b, c \in C[x]$ with the following properties: (i) $r(x) = \phi \frac{a(x+1)}{a(x)} \frac{b(x)}{c(x+1)}$, (ii) $\gcd(b(x), c(x+i)) = 1$ for all positive integers i, (iii) $\gcd(a(x), c(x)) = \gcd(a(x), b(x)) = 1$.

Hint: Adapt the proof of Lemma 2.74.

8****.** (Marko Petkovšek) Using the previous exercise, show that it is sufficient to search for polynomial solutions in line 6 of Algorithm 2.75.

9****.** (Carsten Schneider) Let u, u' be two divisors of p_0 considered in line 2 of Algorithm 2.75, and suppose that $u = \sigma^k(u')$ for some $k \in \mathbb{Z}$. Show that the hypergeometric solutions found in the iterations for u and u' are equivalent, i.e., one of the iterations can be skipped.

10. Find all hypergeometric solutions of the following recurrence equations:

a. $(x+2)(5x+7)\sigma^2(y) - (15x^2+61x+58)\sigma(y) - 2(2x+3)(5x+12)y = 0$;

b. $x(x+1)(x+2)\sigma^2(y) - 2x(2x+3)^2\sigma(y) + 4(x+1)(2x+1)(2x+3)y = 0$;

c. $(x+2)^3\sigma^2(y) - (2x+3)(17x^2+51x+39)\sigma(y) + (x+1)^3 y = 0$;

d. $(5x+8)(20x+39)\sigma^2(y) - 4(100x^2+505x+537)\sigma(y) + 4(5x+18)(20x+59)y = 0$.

11***.** Let $y_1, \ldots, y_n$ be hypergeometric terms that are pairwise not similar.

a. Show that $y_1, \ldots, y_n$ are linearly independent over $C(x)$.

b. Show that if some nontrivial $C(x)$-linear combination of $y_1, \ldots, y_n$ is a solution of a recurrence $p_0 y + \cdots + p_r \sigma^r(y) = 0$, then also one of the y_i is a solution.

12*. Develop an algorithm which for given $p_0, \dots, p_r \in C(x)$ and a given hypergeometric term h over $C(x)$ finds all hypergeometric solutions of the inhomogeneous recurrence

$$p_0 y + \cdots + p_r \sigma^r(y) = h.$$

Use your algorithm and the previous exercise to show that the sum $\sum_{k=0}^{n} \binom{2k}{k}$ cannot be expressed as a linear combination of hypergeometric terms.

13. Find all $\alpha \in \mathbb{Q}$ for which the equation $(x+1)f(x) - \alpha(2x+3)f(x+1) + (x+2)f(x+2) = 0$ has a hypergeometric solution.

14*. Prove or disprove: For every $p_0, \dots, p_r \in C(x)$ the set of all solutions in $C((q))^{\mathbb{Z}}$ of the deformed equation $p_0(x+q)f(x) + \cdots + p_r(x+q)f(x+r) = 0$ with nonnegative valuation growth forms a $C((q))$-subspace of the solution space.

15*. Suppose that C is algebraically closed, and let y be a kernel with valuation growth 0 on all classes $\alpha + \mathbb{Z} \subseteq C$. Show that $\sigma(y)/y \in C$.

16. Find all d'Alembertian solutions of the following recurrences:
a. $(n+1)^2 f(n) - (2n^2+6n+5)f(n+1) + (n+2)^2 f(n+2) = 0$;
b. $2(n+2)(2n+1)f(n) - (n+1)(5n+8)f(n+1) + (n+1)(n+2)f(n+2) = 0$;
c. $2(n+2)(2n+5)f(n) - (n+1)(n+3)(4n+11)f(n+1) + (n+1)(n+2)(5n+14)f(n+2) - (n+1)(n+2)(n+3)f(n+3) = 0$;
d. $(2n+5)(n+1)^2 f(n) - (2n+3)(3n^2+12n+11)f(n+1) + (2n+5)(3n^2+12n+11)f(n+2) - (n+3)^2(2n+3)f(n+3) = 0$.

17. Let $P = \cdots (v_3 S - u_3)(v_2 S - u_2)(v_1 S - u_1)$ be a recurrence operator with coefficients in $C[x]$. Suppose that none of the v_i and u_i have roots in $\mathbb{N}$. For each $i = 1, 2, 3, \dots$, let h_i be a hypergeometric sequence with $(v_i S - u_i) \cdot h_i = 0$. Show that the d'Alembertian solutions

$$\begin{aligned}
a_1(n) &= h_1(n), \\
a_2(n) &= h_1(n) \sum_{k=0}^{n-1} \frac{h_2(k)}{u_1(k)h_1(k)}, \\
a_3(n) &= h_1(n) \sum_{k=0}^{n-1} \left(\frac{h_2(k)}{u_1(k)h_1(k)} \sum_{i=0}^{k-1} \frac{h_3(i)}{u_2(i)h_2(i)} \right), \\
&\vdots
\end{aligned}$$

of P are linearly independent over C.
Hint: We have $(v_{i-1} S - u_{i-1}) \cdots (v_1 S - u_1) \cdot a_i = h_i$ for $i = 1, 2, \dots$

References

Petkovšek presented his algorithm in [354]. The algorithm, which is covered in several textbooks [268, 283, 284, 356], was motivated by Gosper's work on hypergeometric summation, which we discuss in Sect. 5.1. The notions of kernel and shell were introduced by Abramov and Petkovšek in [17]. This terminology motivates the variant of Petkovšek's algorithm given as Algorithm 2.75 in the text. A version of Petkovšek's algorithm for the q-shift case is due to Abramov, Paule, and Petkovšek [22].

Algorithm 2.82 is due to van Hoeij [445]. This algorithm was motivated by a classical method for finding hyperexponential solutions of differential equations (cf. Sect. 3.6). Cluzeau and van Hoeij discuss the use of homomorphic images in this algorithm [161]. Algorithms for finding hypergeometric solutions can be generalized to algorithms for finding so-called m-hypergeometric solutions. A sequence is called m-hypergeometric if it satisfies a recurrence of the form $p(x)f(x+m) - q(x)f(x) = 0$ for some fixed $m \in \mathbb{N} \setminus \{0\}$. The case $m = 1$ amounts to the hypergeometric case as discussed in this section. For the case $m > 1$, see [5, 239, 355, 376, 421] and the references given there.

D'Alembertian solutions of recurrences and differential equations are discussed by Abramov and Petkovšek [15]. Solutions of more general form which can be expressed with summation and product signs can be discovered using techniques from difference Galois theory [125, 234, 440]. The most recent milestone in this direction is an algorithm due to Abramov, Bronstein, Petkovšek and Schneider which can find all hypergeometric solutions of a homogeneous recurrence whose coefficients are given by expressions involving summation and product signs rather than plain rational functions [26].

Chapter 3
The Differential Case in One Variable

3.1 Evaluation

By definition, a D-finite function is a solution of a linear differential equation with polynomial coefficients. In general, we do not necessarily mean a function in the strictest sense but may also regard more formal objects as D-finite "functions", similar to how we speak of rational functions (even though they are just quotients of polynomials) or generating functions (even though they are just formal power series). In general, the actual type of object of a D-finite function depends on the context.

It is only meaningful to ask for the value of a function at a certain point if the function is (or at least can be interpreted as) a function in the usual sense. This shall be the viewpoint adopted in the present section. For a given D-finite function $f: U \to \mathbb{C}$ defined on some open subset U of $\mathbb{C}$, typically (and without loss of generality) a neighborhood of zero, we want to compute the value $f(\xi)$ for some given $\xi \in U$.

What can we expect? If we evaluate the exponential function $f = \exp$ at the point $\xi = 1$, what should be the output of an evaluation algorithm? We might expect to see a symbolic expression representing the constant e. In general, we might expect an expression in terms of well-known constants such as e, π, γ, $\zeta(3)$, $\log(2)$, etc. But such expressions may not exist, and even in very simple examples, it is often not known whether such an expression exists or not.

No algorithms are known which compute the values of D-finite functions in closed form, for any reasonable notion of closed form. But there are algorithms evaluating D-finite functions numerically to any desired (but finite) precision. This is the problem we want to address in the present section: given a D-finite function $f: U \to \mathbb{C}$, defined through a linear differential equation with coefficients in $C[x]$ and initial values in C, and given a point $\xi \in C \cap U$, and given $N \in \mathbb{N}$, find $\eta \in C$ such that $|\eta - f(\xi)| < 10^{-N}$. As always, C is a computable field. In the

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1_3

present section, it is assumed to be a subfield of $\mathbb{C}$. Natural choices are $C = \mathbb{Q}$ and $C = \mathbb{Q}(\mathrm{i})$.

For simplicity, we restrict to the case where 0 is not a root of the coefficient of the highest order derivative in the defining equation. In this case, for any choice of r initial values there is precisely one power series solution of a linear differential equation of order r.

Theorem 3.1 *Let $p_0, \ldots, p_r \in C[x]$ with $x \nmid p_r$ and let $\alpha_0, \ldots, \alpha_{r-1} \in C$. Then there exists exactly one $f = \sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ with $f(0) = \alpha_0, \ldots, f^{(r-1)}(0) = \alpha_{r-1}$ and $p_0 f + \cdots + p_r f^{(r)} = 0$.* □

Proof Write the differential equation in the form

$$f^{(r)}(x) = -\frac{p_0(x)}{p_r(x)} f(x) - \cdots - \frac{p_{r-1}(x)}{p_r(x)} f^{(r-1)}(x).$$

By the assumption $x \nmid p_r$, all of the rational functions on the right hand side can be expanded as power series, say $-\frac{p_i(x)}{p_r(x)} = \sum_{n=0}^{\infty} b_{i,n} x^n$ for certain $b_{i,n} \in C$. Using $f^{(i)}(x) = \sum_{n=0}^{\infty} a_{n+i} (n+i)^{\underline{i}} x^n$ $(i = 0, \ldots, r)$ and equating coefficients of x^n on both sides gives the equation

$$(n+r)^{\underline{r}} a_{n+r} = \sum_{i=0}^{r-1} \sum_{k=0}^{n} a_{k+i} (k+i)^{\underline{i}} b_{i,n-k}.$$

This recurrence extends every choice $a_0, \ldots, a_{r-1}$ of initial values to a unique infinite sequence, and a sequence $(a_n)_{n=0}^{\infty}$ satisfies this recurrence if and only if $\sum_{n=0}^{\infty} a_n x^n$ is a solution of the differential equation. ■

Example 3.2 The differential equation $2(x+1)(3x+4) f''(x) + 3(x+2) f'(x) - 3f(x) = 0$ together with the initial values $f(0) = 1$, $f'(0) = -\frac{1}{2}$ defines a unique formal power series, the coefficients of which can be computed by the formulas in the proof of the theorem above. We obtain

$$f(x) = 1 - \tfrac{1}{2}x + \tfrac{3}{8}x^2 - \tfrac{5}{16}x^3 + \tfrac{35}{128}x^4 - \tfrac{63}{256}x^5 + \tfrac{231}{1024}x^6 \pm \cdots .$$

□

Using the recurrence in the proof of the theorem, we can also derive a bound on how fast the coefficient sequence $(a_n)_{n=0}^{\infty}$ of a formal power series can possibly grow. It turns out that it grows slowly enough to imply convergence for any value of x which is closer to zero than any root of the leading coefficient polynomial p_r.

The proof uses the explicit knowledge we have about the sequences $(b_{i,n})_{n=0}^{\infty}$. As they arise from series expansions of rational functions, we can express them as linear combinations of exponential sequences with polynomial coefficients (cf. Exercise 15 of Sect. 1.1). The exponential terms are precisely the reciprocals of the roots of p_r. Therefore, if ϕ is any positive number such that $\phi > |1/\zeta|$ for every root $\zeta \in \mathbb{C}$ of p_r, then we can find $M \in \mathbb{R}$ such that $|b_{i,n}| \leq \max(M, \phi^n)$ for all $n \in \mathbb{N}$. The rest is a calculation.

Theorem 3.3 *Suppose that $C \subseteq \mathbb{C}$. Let $p_0, \dots, p_r \in C[x]$ with $x \nmid p_r$ and let $f = \sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ be such that*

$$p_0 f + \cdots + p_r f^{(r)} = 0.$$

Let $\xi \in \mathbb{C}$ be such that $|\xi| < |\zeta|$ for every root ζ of p_r. Then the power series f converges for $x = \xi$. □

Proof It suffices to consider the case $r \geq 2$ (see Exercise 1 for $r = 1$). Without loss of generality, suppose that $|\zeta| \leq 1$ for all roots ζ of p_r. If this is not the case, this situation can be achieved by applying a change of variables $x \rightsquigarrow \alpha x$ to the differential equation.

Let ϕ be such that $|\xi| < 1/\phi < |\zeta|$ for all roots ζ of p_r. In order to show that the series $\sum_{n=0}^{\infty} a_n \xi^n$ converges, we show that there is a constant c such that $|a_n| \leq c\phi^n$ for all n, so that $|a_n \xi^n| \leq c|\phi\xi|^n$ for all $n \in \mathbb{N}$ which by $|\phi\xi| < 1$ implies the convergence.

Let $b_{i,n}$ be as in the previous proof, and let $M \in \mathbb{R}$ be such that $|b_{i,n}| \leq \max(M, \phi^n)$ for all $n \in \mathbb{N}$. Because of $\phi > 1/|\zeta| \geq 1$, there will be some $n_0 \in \mathbb{N}$ such that $|b_{i,n}| \leq \phi^n$ for all $n \geq n_0$.

Let $n \in \mathbb{N}$ and c be such that $|a_k| \leq c\phi^k$ for all $k \leq n+r-1$. Then the recurrence

$$(n + r)^{\underline{r}} a_{n+r} = \sum_{i=0}^{r-1} \sum_{k=0}^{n} a_{k+i} (k + i)^{\underline{i}} b_{i,n-k}$$

implies

$$\begin{aligned}
|a_{n+r}| &\leq \frac{1}{(n + r)^{\underline{r}}} \sum_{i=0}^{r-1} \sum_{k=0}^{n} \underbrace{|a_{k+i}|}_{\leq c\phi^{k+i}} (k + i)^{\underline{i}} \underbrace{|b_{i,n-k}|}_{\leq \max(M,\phi^{n-k})} \\
&\leq c \frac{1}{(n + r)^{\underline{r}}} \sum_{i=0}^{r-1} \sum_{k=0}^{n} (k + i)^{\underline{i}} \max(M, \phi^{n-k}) \phi^{k+i} \\
&\leq c \frac{1}{(n + r)^{\underline{r}}} \sum_{i=0}^{r-1} \Bigg(\underbrace{\sum_{k=0}^{n} (k + i)^{\underline{i}} \phi^{n+r}}_{= \frac{1}{i+1} (n + i + 1)^{\underline{i+1}} \phi^{n+r}} + \underbrace{\sum_{k=n-n_0+1}^{n} (k + i)^{\underline{i}} M \phi^{k+i}}_{\leq (n_0 + 1) M (n + i)^{\underline{i}} \phi^{n+r}} \Bigg) \\
&\leq c\phi^{n+r} \sum_{i=0}^{r-1} \Big(\frac{1}{i + 1} \frac{(n + i + 1)^{\underline{i+1}}}{(n + r)^{\underline{r}}} + (n_0 + 1) M \frac{(n + i)^{\underline{i}}}{(n + r)^{\underline{r}}} \Big).
\end{aligned}$$

For $n \to \infty$, this sum approaches $1/r < 1$, because the denominator polynomial dominates all numerator polynomials except when $i = r - 1$, where the first term cancels to $1/r$ and the second term tends to zero. Therefore, there exists $n_1 \in \mathbb{N}$ such that for all $n \geq n_1$ the sum is at most 1, so for these n we can conclude $|a_{n+r}| \leq c\phi^{n+r}$.

Taking $c = \max_{i=0}^{n_1+r-1} |a_i|/\phi^i$ to ensure that $|a_n| \leq c\phi^n$ for all $n \leq n_1 + r - 1$, the calculation above implies inductively that $|a_n| \leq c\phi^n$ for all $n \in \mathbb{N}$. ∎

When ξ is inside the disk of convergence, we can compute the value of $f(\xi)$ to any desired accuracy using the convergent series solutions. From the estimate $|a_n| \leq c\phi^n$ we get

$$|f(\xi) - \sum_{n=0}^{K-1} a_n\xi^n| \leq \sum_{n=K}^{\infty} |a_n\xi^n| \leq \sum_{n=K}^{\infty} c|\phi\xi|^n = \frac{c}{1 - |\phi\xi|}|\phi\xi|^K.$$

Therefore, in order to obtain an evaluation with N correct decimal digits, it suffices to truncate the series at the Kth term, where K is chosen such that $\frac{c}{1-|\phi\xi|}|\phi\xi|^K < 10^{-N}$. Note that such a K not only "exists", but it can be easily computed, because we can compute c and ϕ. To get a suitable choice for ϕ, it suffices to be able to determine the location of the roots of p_r, which can certainly be done. For computing c, observe that, using the notation from the proof of Theorem 3.3, the quantities M and n_0 can be computed from the explicit expressions of the $b_{i,n}$. Then, the index n_1 can be computed from the sum expression (which in concrete examples is just a certain rational function in n). Finally, c can be computed once we know n_1.

Example 3.4 The formal power series f of Example 3.2 converges for all ξ with $|\xi| < 1$. Let us compute $f(\xi)$ for $\xi = \frac{99}{100}$ to 50 decimal digits.

Write the differential equation in the form

$$f''(x) = \frac{3}{2(x+1)(3x+4)} f(x) - \frac{3(x+2)}{2(x+1)(3x+4)} f'(x).$$

By partial fraction decomposition, we can find that the rational function coefficient of $f(x)$ is equal to $\sum_{n=0}^{\infty} b_{0,n}x^n$ with $b_{0,n} = \frac{3}{2}(-1)^n - \frac{9}{8}(-\frac{3}{4})^n$ $(n \in \mathbb{N})$ and the rational function coefficient of $f'(x)$ is equal to $\sum_{n=0}^{\infty} b_{1,n}x^n$ with $b_{1,n} = -\frac{3}{2}(-1)^n + \frac{3}{4}(-\frac{3}{4})^n$ $(n \in \mathbb{N})$.

We have $|b_{i,n}| \leq \frac{3}{2}$ for $i = 0, 1$ and all $n \in \mathbb{N}$. Therefore, we can take $M = \frac{3}{2}$ and $n_0 = 0$, regardless of the choice of ϕ. Next, we have to find n_1 such that for all $n \geq n_1$ the sum

$$\sum_{i=0}^{r-1} \left(\frac{1}{i+1} \frac{(n+i+1)^{\underline{i+1}}}{(n+r)^{\underline{r}}} + (n_0+1)M \frac{(n+i)^{\underline{i}}}{(n+r)^{\underline{r}}} \right)$$

is bounded by 1. With $r = 2$ and M and n_0 from above, the sum simplifies to $(n^2 + 8n + 10)/(2n^2 + 6n + 4)$, which is bounded by 1 for $n \geq 4$. So we can take $n_1 = 4$.

We choose $\phi = 1 + 10^{-7}$. (Any other value slightly larger than 1 would also work.) Then $c = \max_{i=0}^{n_1+r-1} |a_i|/\phi^i = 1$.

Now in order to guarantee an accuracy of 50 decimal digits, we choose the number K of series terms such that

$$\frac{1}{1 - |(1 + 10^{-7})\frac{99}{100}|}((1 + 10^{-7})\frac{99}{100})^K < 10^{-51}.$$

Any number $K \geq \frac{\log(10^{-51}(1-|(1+10^{-7})\frac{99}{100}|))}{\log((1+10^{-7})\frac{99}{100})} \approx 12142.7$ will do the job. We finally obtain

$$\begin{aligned} f(\tfrac{99}{100}) &\approx \sum_{n=0}^{12143} a_n (\tfrac{99}{100})^n \\ &= \frac{3612752311(\ldots\text{ 31571 digits suppressed }\ldots)4727152463}{5096414302(\ldots\text{ 31571 digits suppressed }\ldots)0000000000} \\ &\approx 0.70888120500833590076543536135061942100194513212079607390 36. \end{aligned}$$

In this example, the correct value is $10/\sqrt{199}$, and the approximation turns out to be correct not only to 50 but even to 56 digits. Of course, if performance matters, the whole calculation should be done with approximate numbers rather than with rational numbers. □

In order to ensure that the evaluation of f is correct to N digits, the estimates above suggest to use a number K of series terms which is linear in N. It is possible, though not advisable, to use the recurrence equation in the proofs of Theorems 3.1 and 3.3 for computing these terms. A more efficient way is to exploit that coefficient sequences of D-finite power series are themselves D-finite as sequences.

Theorem 3.5 *(See Theorem 2.33 for a converse) Let $p_0, \ldots, p_r \in C[x]$ be polynomials of degree at most d, define $p_{i,j} = [x^j]p_i$ for $i = 0, \ldots, r$ and $j \in \mathbb{Z}$, so that $p_i = \sum_{j\in\mathbb{Z}} p_{i,j}x^j$.*

A (possibly bilateral) series $f(x) = \sum_{n=-\infty}^{\infty} a_n x^n$ satisfies the differential equation

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = 0$$

if and only if its coefficient sequence $(a_n)_{n=-\infty}^{\infty} \in C^{\mathbb{Z}}$ satisfies the recurrence equation

$$q_0(n)a_n + \cdots + q_{r+d}(n)a_{n+r+d} = 0,$$

where $q_k = \sum_{i=0}^{r} p_{i,d+i-k}(x+k)^{\underline{i}}$ *(*$k = 0, \ldots, r+d$*).*

In particular, if $f(x) = \sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ *satisfies a linear differential equation of order* r *with polynomial coefficients of degree at most* d*, then* $(a_n)_{n=0}^{\infty} \in C^{\mathbb{N}}$ *satisfies a linear recurrence equation of order* $r+d$ *with polynomial coefficients of degree at most* r*.* □

Proof For every series $f(x) = \sum_{n=-\infty}^{\infty} a_n x^n$ and every $i \in \mathbb{N}$ we have $f^{(i)}(x) = \sum_{n=-\infty}^{\infty} a_{n+i}(n+i)^{\underline{i}} x^n$. Therefore,

$$\begin{aligned}
&\sum_{i=0}^{r}\sum_{j\in\mathbb{Z}}\sum_{n\in\mathbb{Z}} p_{i,j} a_{n+i}(n+i)^{\underline{i}} x^{n+j} = 0 \\
\iff\ &\sum_{n\in\mathbb{Z}}\sum_{i=0}^{r}\sum_{j\in\mathbb{Z}} p_{i,j} a_{n-j+i}(n-j+i)^{\underline{i}} x^{n} = 0 \\
\iff\ &\forall\, n \in \mathbb{Z} : \sum_{i=0}^{r}\sum_{j\in\mathbb{Z}} p_{i,j}(n-j+i)^{\underline{i}} a_{n-j+i} = 0 \\
\iff\ &\forall\, m \in \mathbb{Z} : \sum_{k\in\mathbb{Z}}\sum_{i=0}^{r} p_{i,d+i-k}(m+k)^{\underline{i}} a_{m+k} = 0.
\end{aligned}$$

In the last step, besides exchanging the order of summation, we have applied the substitutions $j = d+i-k$ and $n = m+d$. Note that $\sum_{i=0}^{r} p_{i,d+i-k}(x+k)^{\underline{i}} = 0$ for $k < 0$ or $k > d+r$.

This proves the claimed equivalence. The remaining statement is a direct consequence if we view a power series $\sum_{n=0}^{\infty} a_n x^n \in C[[x]]$ as a bilateral series $\sum_{n=-\infty}^{\infty} a_n x^n$ with $a_n = 0$ for $n < 0$. ■

Theorem 3.5 reduces the computation of series coefficients of D-finite power series to the computation of terms of D-finite sequences, which was discussed in Sect. 2.1. Furthermore, we have seen in Sect. 2.3 that if $(a_n)_{n=0}^{\infty}$ is D-finite, then so is $(\sum_{k=0}^{n} k^{\underline{i}} a_k \xi^{k-i})_{n=0}^{\infty}$ for any constant ξ and any $i \in \mathbb{N}$. So instead of computing K terms of the sequence $(a_n)_{n=0}^{\infty}$ and then adding them up, we can just compute the Kth term of the sequence of partial sums. With Algorithm 2.2 in Sect. 2.1 it is possible to efficiently compute the Kth term of a D-finite sequence without computing all of the previous terms.

Example 3.6 The differential equation $2(x+1)(3x+4)f''(x) + 3(x+2)f'(x) - 3f(x) = 0$ translates into the recurrence

$$3(n-1)(2n+1)a_n + 2(n+1)(7n+3)a_{n+1} + 8(n+1)(n+2)a_{n+2} = 0.$$

For the partial sums $s_n = \sum_{k=0}^{n} a_n \xi^n$, we obtain the recurrence

$$
\begin{aligned}
&3n(2n+3)\xi s_n - (-14n^2\xi + 6n^2 - 48n\xi + 9n - 40\xi)s_{n+1} \\
&+ 2(n+2)(4n\xi - 7n + 12\xi - 10)s_{n+2} - 8(n+2)(n+3)s_{n+3} = 0. \qquad \square
\end{aligned}
$$

For a fixed D-finite function f and a fixed evaluation point ξ inside the disk of convergence, the computation of $f(\xi)$ to N decimal digits requires the computation of the Kth term of a D-finite sequence, where $K = \mathrm{O}(N)$. Therefore, the cost amounts to $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(N)\log(N)^2)$ bit operations, where $\mathrm{M}_{\mathbb{Z}}$ is the cost for integer multiplication. There is not much room for improving the O-estimate, but we can do something to improve the constant factor hidden in the O.

One observation is that evaluating close to the boundary of the disk of convergence is more costly than close to the center. If we are faced with an evaluation point close to the boundary, an idea is to choose an alternative expansion point. Choosing some point ζ instead of 0 as a new expansion point means computing approximations of $f(\zeta), \dots, f^{(r-1)}(\zeta)$ and using these as the initial values. Note that we can compute approximations of the derivatives in a similar way as approximations of the function itself. For example, for the first derivative we have

$$
|f'(\zeta) - \sum_{n=0}^{K-1} n a_n \zeta^{n-1}| \le \sum_{n=K}^{\infty} nc|\phi\zeta|^n/|\zeta| = \frac{c(|\phi\zeta| + (1-|\phi\zeta|)K)}{(1-|\phi\zeta|)^2|\zeta|}|\phi\zeta|^K.
$$

In general, for evaluating the ith derivative, there is a bivariate polynomial p_i such that the error is bounded by

$$
\frac{cp_i(K, |\phi\zeta|)}{(1-|\phi\zeta|)^{i+1}|\zeta|^i}|\phi\zeta|^K,
$$

and it is not hard to determine these polynomials (Exercise 6). With the results of Sect. 2.1, we can determine to which accuracy the initial values have to be computed in order to be safe against error propagation.

Example 3.7 Consider again the function f defined by $2(x+1)(3x+4)f''(x) + 3(x+2)f'(x) - 3f(x) = 0$ and $f(0) = 1$ and $f'(0) = -1/2$. We want to compute again $f(99/100)$ to 50 decimal digits, but this time we first change the expansion point to $\zeta = 1/2$.

Setting $g(x) = f(x+1/2)$, the differential equation for f translates into the equation $(2x+3)(6x+11)g''(x) + 3(2x+5)g'(x) - 6g(x) = 0$, and computing $f(99/100)$ is the same as computing $g(49/100)$. Writing $g(x) = \sum_{n=0}^{\infty} b_n x^n$, the differential equation for g translates into the recurrence

$$
\begin{aligned}
&3300(n+2)(n+3)s_{n+3} + (n+2)(2383n+649)s_{n+2} \\
&- 5(152n^2 + 963n + 1078)s_{n+1} - 294n(2n+3)s_n = 0
\end{aligned}
$$

for the partial sums $s_n = \sum_{k=0}^{n} b_k (\frac{49}{100})^k$.

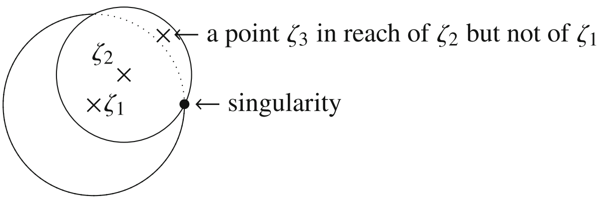
Reasoning as in Example 3.4, we find that already the approximation s_{100} will be correct to 50 decimal digits. Note that 100 is considerably smaller than 12143. However, we still need to compute the initial values s_0, s_1, s_2 by evaluating f and its derivatives at $\zeta = 1/2$. An application of Proposition 2.5 suggests that we should compute these terms to a 62-decimal-digit accuracy in order to get s_{100} correct to 50 decimal digits. The initial values are essentially $f(1/2)$, $f'(1/2)$ and can be computed to a 62 decimal digits as in Example 3.4. It turns out that the respective series can already be truncated after 200 terms. □

If the evaluation point is not just close to the boundary of the disk of convergence but in fact close to a root of p_r, it may be necessary to change the expansion point several times in order to obtain a good overall performance. In such situations, it can be useful to determine *transition matrices* that translate the initial values at some point to initial values at some other point. Given a differential equation of order r and $\zeta_1, \zeta_2 \in \mathbb{C}$ such that ζ_1 is not a root of the leading coefficient polynomial and ζ_2 is inside the disk of convergence of any formal power series solution about ζ_1, there is a matrix $T_{\zeta_1 \to \zeta_2} \in \mathbb{C}^{r \times r}$ with

$$\begin{pmatrix} f(\zeta_2) \\ f'(\zeta_2) \\ \vdots \\ f^{(r-1)}(\zeta_2) \end{pmatrix} = T_{\zeta_1 \to \zeta_2} \begin{pmatrix} f(\zeta_1) \\ f'(\zeta_1) \\ \vdots \\ f^{(r-1)}(\zeta_1) \end{pmatrix}$$

for every solution f of the differential equation. This matrix is called the transition matrix for ζ_1 and ζ_2. We have $T_{\zeta_1 \to \zeta_3} = T_{\zeta_2 \to \zeta_3} T_{\zeta_1 \to \zeta_2}$ whenever $\zeta_1, \zeta_2, \zeta_3$ are such that all three matrices are well defined. The entries of a transition matrix $T_{\zeta_1 \to \zeta_2}$ can be computed as illustrated in the examples above. For example, the ith row of $T_{\zeta_1 \to \zeta_2}$ is the vector $(f(\zeta_2), \ldots, f^{(r-1)}(\zeta_2))$ where f is the solution defined by the initial values $f^{(i)}(\zeta_1) = 1$ and $f^{(j)}(\zeta_1) = 0$ for all $j \in \{0, \ldots, r-1\} \setminus \{i\}$. Note that the entries of a transition matrix can usually not be determined exactly but only up to some arbitrary (but finite) precision.

When we switch from one expansion point to another, the disk of convergence around the new expansion point may cover points that are not covered by the original expansion point:



Therefore, changing the expansion point is not only interesting for performance reasons but also allows us to evaluate a function outside its disk of convergence.

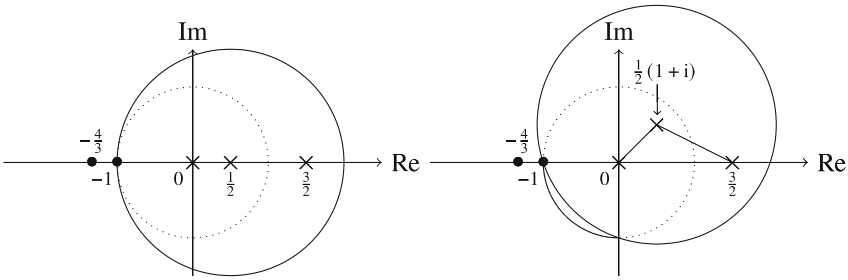
It is a fundamental fact in complex analysis that by finitely many changes of the expansion point, we can reach any point of the complex plane that is not a root of the leading coefficient polynomial p_r of the differential equation. This is known as *analytic continuation.* Moreover, the value at the target point does not depend on the precise path taken from the original expansion point but only on the homotopy class in $\mathbb{C} \setminus \{\xi : p_r(\xi) = 0\}$. This means the value won't change if we wiggle the path a bit, as long as we do not touch any root of p_r by the wiggling. In other words, what matters is only on which side of the root of p_r we pass.

Example 3.8 We continue with the function f already considered in the previous examples.

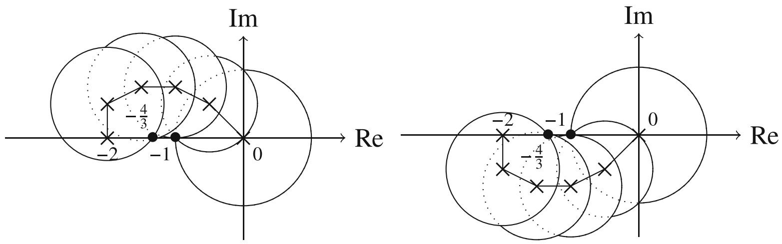
1. In Example 3.7, we have changed the expansion point to $\zeta_2 = 1/2$. The disk of convergence around this point has radius $3/2$, so it includes the point $\zeta_3 = 3/2$ which is not contained in the disk of convergence centered at $\zeta_1 = 0$, which has radius 1. Using the first 270 terms of the series about $1/2$ gives

$$f(3/2) \approx 0.63245553203367586639977870888654370674391102786508,$$

which is correct to 50 decimal digits.
Alternatively, we could change the expansion point from 0 to $\zeta_2 = (1 + \mathrm{i})/2$, because $(1 + \mathrm{i})/2$ belongs to the disk of convergence around 0 and $3/2$ belongs to the disk of convergence around $(1 + \mathrm{i})/2$. Doing so yields the same result, but it turns out that in this case 320 series terms are needed to reach an accuracy of 50 decimal digits.



2. For evaluating f at -2, we do not have the option to take a straight path from 0 to -2, because the singularities at -1 and $-4/3$ are in the way. The value of f differs depending on whether we take a path above or below the critical points. In the first case, we obtain the result $0 - \mathrm{i}$ to 50 decimal digits, while in the second case we get $0 + \mathrm{i}$ to 50 decimal digits.



□

The evaluation procedure as described so far can be summarized as follows.

Algorithm 3.9
Input: *A D-finite function f defined by a differential equation* $p_0 f + \cdots + p_r f^{(r)} = 0$ *with polynomials* $p_0, \ldots, p_r \in C[x]$ *and initial values* $f(\zeta_0), \ldots, f^{(r-1)}(\zeta_0) \in C$ *at some point* $\zeta_0 \in C$; *numbers* $\zeta_1, \ldots, \zeta_s \in C$ *such that no line segment connecting* ζ_i *to* ζ_{i+1} $(i = 0, \ldots, s-1)$ *contains a root of* p_r; *a number* $N \in \mathbb{N}$.
Output: *The values* $f(\zeta_s), \ldots, f^{(r-1)}(\zeta_s) \in \mathbb{C}$ *according to the analytic continuation* $\zeta_0 \to \cdots \to \zeta_s$, *to an accuracy of N decimal digits.*

1 *If* $s = 0$, *return* $f(\zeta_0), \ldots, f^{(r-1)}(\zeta_0)$.
2 *while* $|\zeta_{s-1} - \zeta_s| > \min_{\xi : p_r(\xi)=0} |\zeta_{s-1} - \xi|$ *do*
3 *Set* $\zeta_{s+1} = \zeta_s$, $\zeta_s = \frac{1}{2}(\zeta_{s+1} + \zeta_{s-1})$, *and* $s = s + 1$.
4 *Construct recurrences for the truncated series solutions* $s_n^{(i)} = \sum_{k=0}^{n} a_{k+i}(k+1)^{\overline{i}}(x - \zeta_{s-1})^k$ *of the ith derivatives* $(i = 0, \ldots, r-1)$ *of a solution of the differential equation.*
5 *Determine a bound* $\sigma > 0$ *on the largest singular values of the companion matrices for* $n \in \mathbb{N}$ *of these recurrences.*
6 *Determine a* $K \in \mathbb{N}$ *such that* $|f^{(i)}(\zeta_s) - \sum_{k=0}^{K} a_{k+i}(k+1)^{\underline{i}}(\zeta_s - \zeta_{s-1})^k| < 10^{-N}$ *for* $i = 0, \ldots, r-1$.
7 *Compute* $f(\zeta_{s-1}), \ldots, f^{(r-1)}(\zeta_{s-1})$ *to* $\lceil N + K \log_{10} \sigma \rceil$ *decimal digits accuracy by calling this algorithm recursively.*
8 *If the recurrences determined in line 4 have order larger than r, compute a few more derivatives* $f^{(i)}(\zeta_{s-1})$ *via the differential equation.*
9 *Using the recurrences from line 4 with the approximations* $a_i = f^{(i)}(\zeta_{s-1})/i!$ *as initial values, compute* $s_K^{(0)}, \ldots, s_K^{(r-1)}$ *and return these numbers.*

Theorem 3.10 *Algorithm 3.9 is correct. If* f *and* $\zeta_0, \ldots, \zeta_s$ *are fixed and only N varies, it requires* $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(N)\log(N)^2)$ *bit operations.* □

Proof Correctness follows directly from how the various bounds are chosen and how the values $f(\zeta_s), \ldots, f^{(r-1)}(\zeta_s)$ are defined.

For the complexity claim, observe that only lines 6, 7, and 9 depend on N. The computation time for line 6 is negligible, and for the resulting K we can assume $K = \mathrm{O}(N)$ according to the formulas given earlier in this section. The computation in line 9 takes $O(M_{\mathbb{Z}}(K)\log(K)^2)$ bit operations by the results of Sect. 2.1. For the recursive call in line 7, observe that the depth of the recursion only depends on the path but not on N. Therefore, the total number of executions of line 9 does not depend on N. Moreover, although N gets increased for the recursive call, we still request only $O(N)$ correct digits at each recursive level. Altogether, we do $O(1)$ many evaluations of a certain K-th sequence term with $K = O(N)$, each costing $O(M_{\mathbb{Z}}(K)\log(K)^2)$. Taking into account that $M_{\mathbb{Z}}(O(N)) = O(M_{\mathbb{Z}}(N))$, the claimed complexity bound follows. ■

Like earlier, instead of considering a particular solution of the differential equation, we can use transition matrices to describe the change of an expansion point for all solutions of the equation. We use the notation $T_{\zeta_1 \xrightarrow{\gamma} \zeta_2}$ for the transition matrix representing the change from expansion point ζ_1 to expansion point ζ_2 via analytic continuation along the path γ connecting these two points. As shown in the example above, the choice of γ matters. The path can even make a difference if ζ_2 belongs to the disk of convergence centered at ζ_1, as shown in Exercise 12.

Although the precise path has no influence on the result, it does affect the computation time. In general, a good path is one that does not get too close to the roots of p_r and does not consist of too many steps. A good rule of thumb is to choose intermediate points $\zeta_1, \ldots, \zeta_{s-1}$ on a path connecting the (non-negotiable) points ζ_0 and ζ_s in such a way that

$$\sum_{k=0}^{s} \frac{|\zeta_k - \zeta_{k+1}|}{\min_{\xi : p_r(\xi)=0} |\zeta_k - \xi|}$$

is minimized. Note that for the analytic continuation to succeed, it is necessary that each term in this sum is less than 1.

In addition to optimizing the location of the vertices ζ_i, it can also be helpful to replace some vertices with nearby vertices that have smaller bitsizes, because the bit length of the vertices enters into the recurrences for the truncated series used in Algorithm 3.9. For example, $\frac{1}{2}$ will be a better choice than $\frac{1003251345234598796135}{2000158687364582765833}$. Changing the inner vertices of the path is free of charge, as long as the change does not alter the homotopy class of the path. Changing the endpoints is a bit more dangerous. The following theorem clarifies how much change we can allow without being worried about changing the evaluation result.

Theorem 3.11 *Let $f = \sum_{n=0}^{\infty} a_n x^n$ be a power series converging in a neighborhood of zero, let c, ϕ be such that $|a_n| < c\phi^n$ for all $n \in \mathbb{N}$, let $\zeta, \bar{\zeta} \in \mathbb{C}$ be such that $|\zeta|, |\bar{\zeta}| < 1/\phi$ and let $\epsilon > 0$ be such that $|\zeta - \bar{\zeta}| < \epsilon$. Suppose that $|\bar{\zeta}| > |\zeta|$. Then*

$$|f(\zeta) - f(\bar{\zeta})| < \frac{c\epsilon|\phi\bar{\zeta}|}{(1 - |\phi\bar{\zeta}|)^2|\bar{\zeta}|}.$$

□

Proof We have

$$|f(\zeta) - f(\bar{\zeta})| = |\sum_{n=0}^{\infty} a_n \zeta^n - \sum_{n=0}^{\infty} a_n \bar{\zeta}^n| \le \sum_{n=0}^{\infty} c\phi^n |\zeta^n - \bar{\zeta}^n|$$
$$\le \sum_{n=0}^{\infty} c\phi^n |\zeta - \bar{\zeta}| \sum_{k=0}^{n-1} |\zeta^k \bar{\zeta}^{n-1-k}|.$$

By $|\zeta - \bar{\zeta}| < \epsilon$ and $|\zeta| < |\bar{\zeta}|$, the latter is at most

$$c\epsilon \sum_{n=0}^{\infty} \sum_{k=0}^{n-1} |\bar{\zeta}^{n-1}|\phi^n \le c\epsilon \sum_{n=0}^{\infty} n|\bar{\zeta}|^{n-1}\phi^n = \frac{c\epsilon|\phi\bar{\zeta}|}{(1-|\phi\bar{\zeta}|)^2|\bar{\zeta}|},$$

as claimed. ■

According to this theorem, in order to compute $f(\zeta)$ to an accuracy of N decimal digits, we can compute $f(\bar{\zeta})$ to an accuracy of N decimal digits, provided that $\bar{\zeta}$ is such that $|\zeta - \bar{\zeta}| < \frac{|\bar{\zeta}|(1-|\phi\bar{\zeta}|)^2}{c|\phi\bar{\zeta}|} 10^{-N}$. The theorem allows us in particular to compute the value of $f(\zeta)$ at any computable complex numbers ζ. Recall that a real number is called computable if there is an algorithm which for every given N computes the Nth decimal digit. A complex number is computable if its real part and its imaginary part are computable real numbers. Examples for computable numbers are π, e, γ, $\sqrt{2}$, $\log(2)$, and in fact, by Algorithm 3.9, any number $f(\zeta)$ where f is D-finite and $\zeta \in C$.

Example 3.12 Once more, let f be the function defined in Example 3.2. We want to compute $f(1/\pi)$ to 50 decimal digits.

According to Theorem 3.11, we get the right result if we replace $1/\pi$ by the approximation

$$1/\pi \approx 0.31830988618379067153776752674502872406891929148091\,29.$$

In order to compute

$$f(0.3183098861837906715377675267450287240689192914809129)$$

from the expansion at 0, we need to take into account roughly 100 terms of the series. The result is

$$f(1/\pi) \approx 0.8709460333423513246699788685653291116596829815123\,5.$$

□

Using Theorem 3.11, we can evaluate a D-finite function f at a computable number ζ to N digits by choosing a $\bar{\zeta} \in C$ that is sufficiently close to ζ and then calling Algorithm 3.9 with $\bar{\zeta}$ instead of ζ. This is obviously correct, but it is not efficient when N is large. The complexity analysis given in the proof of Theorem 3.10 no longer applies in this situation because it uses the assumption that the recurrences for the truncated series $s_n^{(i)}$ are independent of N. But if the endpoint ζ_s of the path is a computable number and we increase the target accuracy, we will have to also increase the input accuracy of the approximation of ζ_s accordingly, and this number certainly affects the recurrences.

If the coefficients in a recurrence have length L, then Algorithm 2.2 from Sect. 2.1 computes the Kth term of a solution of the recurrence in $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(LK)\log(K)^2)$ bit operations. With $L = \mathrm{O}(N)$ and $K = \mathrm{O}(N)$, this is quadratic in N. Our goal is to bring it back to quasi-linear time by balancing L and K. The idea is to use the phenomenon observed in Example 3.7: we do several changes of the evaluation point and exploit the fact that the series will converge more quickly if we are close to the center of the disk of convergence. Suppose we are given $\zeta_0, \ldots, \zeta_s$ with $\zeta_0, \ldots, \zeta_{s-1} \in C$ and $\zeta_s \in \mathbb{C}$ a computable number. Let $\zeta_s^{(0)} \in C$ be an approximation to ζ_s, sufficiently close so that it is legitimate to insert $\zeta_s^{(0)}$ as an additional vertex into the path and that the leading coefficient polynomial p_r of the differential equation has no root in a small circle containing ζ_s and $\zeta_s^{(0)}$. We choose a sequence $\zeta_s^{(0)}, \zeta_s^{(1)}, \ldots$ that rapidly converges to ζ_s. More precisely, the sequence should be chosen such that each term is at least twice as accurate and at most twice as long as the previous one. For example, a possible choice for $\zeta_s = \pi$ might be:

$$\begin{aligned}
\zeta_s^{(0)} &= 3 \quad (1 \text{ digit}),\\
\zeta_s^{(1)} &= 3.14 \quad (1+2 \text{ digits}),\\
\zeta_s^{(2)} &= 3.141592 \quad (1+2+4 \text{ digits}),\\
\zeta_s^{(3)} &= 3.14159265358979 \quad (1+2+4+8 \text{ digits}),\\
\zeta_s^{(4)} &= 3.1415926535897932384626433832 79 \quad (1+2+4+8+16 \text{ digits}),\\
&\ \ \vdots
\end{aligned}$$

Such a sequence approximates ζ_s quickly in the sense that the $\log(N)$-th term is already accurate to $\mathrm{O}(N)$ digits. Moreover, we have $|\zeta_s^{(k)} - \zeta_s^{(k+1)}| < u10^{-2^k}$ for some constant u and all $k \in \mathbb{N}$, and each $\zeta_s^{(k)}$ has at most $v2^k$ digits for some constant v and all $k \in \mathbb{N}$. In an implementation, it is usually better to use binary digits, which is why the technique is known as *bit bursting* in the literature. However, the base is not essential in theory, and for better readability, let us finish the discussion using decimal digits.

For the computation of the values $f^{(i)}(\zeta_s^{(k)})$ from the values $f^{(i)}(\zeta_s^{(k-1)})$, we need to truncate the various series at some truncation order K with

$$\frac{cp_i(K, |\phi u 10^{-2^k}|)}{(1 - |\phi u 10^{-2^k}|)^{i+1}|u 10^{-2^k}|} |\phi u 10^{-2^k}|^K < 10^{-N},$$

where c and ϕ are the constants from Theorem 3.1 and p_i is the bivariate polynomial from Exercise 6. For the smallest K meeting this requirement we will roughly have $K \approx w_i N/2^k$ for certain constants w_i. Since $L = v2^k$ is also the length of $\zeta_s^{(k)}$, the computation time for computing the Kth term of the truncated series is bounded by $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(LN/L)\log(K)^2) = \mathrm{O}(\mathrm{M}_{\mathbb{Z}}(N)\log(N)^2)$ for each k.

Therefore, in order to calculate $f(\zeta_s)$ efficiently, we replace the given path $\zeta_0, \ldots, \zeta_s$ by

$$\zeta_0, \ldots, \zeta_{s-1}, \zeta_s^{(0)}, \ldots, \zeta_s^{(M)}$$

for some $M \in \mathbb{N}$ such that $|\zeta_s^{(M)} - \zeta_s|$ meets the bound of Theorem 3.11. By the choice of the sequence, we have $M = \mathrm{O}(\log N)$. Applying Algorithm 2.2, we are going to spend $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(N)\log(N)^2)$ bit operations at each recursion level, and since there are now $\mathrm{O}(\log N)$ levels, the total cost for computing $f(\zeta_s)$ to N digits accuracy amounts to $\mathrm{O}(\mathrm{M}_{\mathbb{Z}}(N)\log(N)^3)$ bit operations.

Exercises

1. Prove Theorem 3.3 for $r = 1$.

2*. Let $p_0, \ldots, p_r \in C[x]$, $p_r(0) \neq 0$, and let $g \in C[[x]]$. Show that there exists $f \in C[[x]]$ with $p_0 f + \cdots + p_r f^{(r)} = g$.

3. Show that $\sum_{n=0}^{\infty} x^{2^n} \in C[[x]]$ is not D-finite.

4. Construct a recurrence for the series coefficients of a solution of the differential equation $(x+1)f''(x) + (x+2)f'(x) + (x+3)f(x) = 0$.

5**. Compute the first 100 decimal digits of $\mathrm{e} = \exp(1)$ by evaluating the function f defined by $f''(x) - 2f'(x) + f(x) = 0$ and $f(0) = f'(0) = 1$ at $\xi = 1$.

6. Let $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[x]$ and let $c, \phi \in \mathbb{R}$ be such that $|a_n| \leq c\phi^n$ for all $n \in \mathbb{N}$. Let $\xi \in \mathbb{C}$ be such that $|\xi| < 1/\phi$.

For $i = 2, 3, 4$, determine polynomials $p_i \in \mathbb{Q}[x, y]$ such that for all $K \in \mathbb{N}$ we have $|f^{(i)}(\xi) - \sum_{n=0}^{K-1} n^{\underline{i}} a_n \xi^{n-i}| < \frac{cp_i(K, |\phi\xi|)}{(1-|\phi\xi|)^{i+1}|\xi|} |\phi\xi|^K$.

7. Compute a recurrence for $(a_n)_{n=0}^{\infty}$ when $f(x) = \sum_{n=0}^{\infty} a_n x^n$ is a solution to the following differential equations:

a. $f'(x) - f(x) = 0$;

b. $(1 - x)f'(x) - f(x) = 0$;

c. $x^3 f^{(3)}(x) + 16x^2 f''(x) + 69xf'(x) + 75f(x) = 0$.

8. Let $\sum_{n=0}^{\infty} a_n x^n$ be a formal power series with $|a_n| \le c\phi^n$ for some $c, \phi \in C$ and all $n \in \mathbb{N}$. Let $\xi \in C$ be such that $|\phi\xi| < 1$. Show that there exist $\bar{c}, \bar{\phi} \in C$ such that for any $\xi_0 \in C$ with $|\xi_0| < |\xi|$ the sequence $(b_n)_{n=0}^{\infty}$ defined through $\sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} a_n(\xi_0 + x)^n$ satisfies $|b_n| \le \bar{c}\bar{\phi}^n$ for all $n \in \mathbb{N}$.

9. Show that the Nth decimal digit of π can be computed with $\mathrm{O}^{\sim}(N)$ bit operations.

10. In Example 3.7, how would the truncation orders change if we choose $\zeta = 2/5$ instead of $\zeta = 1/2$ as the intermediate expansion point?

11. The function $f(x) = \log(x + 1)$ satisfies the differential equation $(x + 1)f''(x) + f'(x) = 0$. With this equation and the initial values $f(0) = 0$, $f'(0) = 1$, compute $\log(3)$ to 50 decimal digits.

12. Let f be the function defined by the differential equation and initial values from Example 3.4.

a. What is the value of f at -2 (to 3 decimal digits, say) if a path as indicated below on the left is chosen for analytic continuation?

b. What is the value of f at 0 (to 3 decimal digits, say) if a path as indicated below on the right is chosen for analytic continuation?

13*. It can be shown that if a differential equation has only algebraic solutions, then the eigenvalues of a transition matrix for a closed path are roots of unity. Use this necessary condition to show that the differential equation $(x+1)^2(x+3)f''(x) - (x + 1)f'(x) + 2f(x) = 0$ has at least one transcendental solution.

14. Let f be the function defined by the differential equation and initial values from Example 3.4. Compute $f(\pi)$ to 50 decimal digits.

15. In the setting of Theorem 3.11, derive a bound for $|f'(\zeta) - f'(\bar{\zeta})|$.

16. It was pointed out in the text that if the interior points of a path for analytic continuation are complicated numbers, we can safely replace them by more simple numbers nearby. It was also discussed what to do if the endpoint of the path is a complicated number. What can we do if the startpoint of the path is a complicated number?

17. In the complexity analysis of bit bursting, we tacitly assumed that there is a uniform bound σ (independent of N) on the largest singular value of the companion matrix of the recurrence equations involved. Why is this a fair assumption?

18. In Example 3.7 we have changed the expansion point in order to get a better convergence rate. Another way of getting better convergence is known as *preconditioning.* For evaluating a D-finite function f at a point ζ, we choose a suitable auxiliary function h and set $g = hf$ and then compute $f(\zeta)$ as $g(\zeta)/h(\zeta)$.

Try this approach for the function f of Example 3.7 and the point $\zeta = 99/100$, using $h(x) = \exp(55x)$ as an auxiliary function. How many series terms of g are needed in order to evaluate $f(\zeta)$ to an accuracy of 50 decimal digits?

Hint: The function $g(x) = \exp(55x) f(x)$ is D-finite and satisfies the differential equation $2(x+1)(3x+4)g''(x) + (-660x^2 - 1537x - 874)g'(x) + (18150x^2 + 42185x + 23867)g(x) = 0$.

References

Convergence considerations and analytic continuation are classical concepts of complex analysis, and the results in this section are effective versions of these results. While such effective versions had been formulated for particular functions before, the Chudnovsky brothers [150] gave the first treatment that applies to arbitrary D-finite functions. Essentially the same technique was proposed by van der Hoeven [432]. He generalizes the idea further in [436], where he develops the notion of a computable analytic function. He also proposes fast algorithms for evaluating a D-finite function near or in an isolated singularity [433] and for evaluating a D-finite power series whose radius of convergence is zero [435]. The bit-bursting algorithm is again due to the Chudnovsky brothers [151], see also the book by Brent and Zimmermann [109] and the references given there.

Producing efficient implementations of the algorithms in this section is quite a challenge. The first general such implementation was given by Mezzarobba [323, 324] for Maple. Meanwhile, he also has an efficient implementation for Sage [325]. Besides requiring a sophisticated infrastructure for arbitrary precision arithmetic (cf. the references on ball arithmetic given at the end of Sect. 2.1), the performance of an implementation also crucially depends on the choice of good bounds. In the interest of shorter proofs, we have only discussed quite poor bounds in this section. Better bounds were given by Mezzarobba [326].

3.2 The Solution Space

Instead of an isolated solution of a given differential equation, let us now consider the set of all solutions of a differential equation. We drop the assumption that C be a subfield of $\mathbb{C}$ adopted in the previous section, but maintain the assumption that C has characteristic zero. Note that Theorems 3.1 and 3.5 of the previous section hold for all fields C of characteristic zero.

We are interested in solutions in $C[[x]]$. It is clear that the set of solutions forms a C-vector space, so it's fair to call it the solution space of the equation. It follows from Theorem 3.1 that this space has dimension r whenever x is not a factor of the leading coefficient polynomial p_r. When $x \mid p_r$, the dimension of the solution space is typically smaller than r, but it may still be equal. We will see later in this section (Theorem 3.20) that it can never be larger.

Example 3.13

1. The solution space of $xf'(x) - 5f(x) = 0$ in $C[[x]]$ is generated by $x^5 \in C[[x]]$, so the dimension matches the order despite the fact that $x \mid p_r$.
2. The solution space of $xf'(x) + f(x) = 0$ in $C[[x]]$ is $\{0\}$. One way to see this is via the recurrence associated to the differential equation (cf. Theorem 3.5). It turns out that for any series solution $f(x) = \sum_{n=0}^{\infty} a_n x^n$ we must have $(n + 1)a_n = 0$, which implies $a_n = 0$ for all $n \in \mathbb{N}$. □

It seems that $x \mid p_r$ is a situation which needs special attention. This motivates the following definition.

Definition 3.14 Let $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$. A root $\xi \in \bar{C}$ of $p_r \in C[x] \setminus \{0\}$ is called a *singularity* of the differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$. A point $\xi \in \bar{C}$ which is not a singularity is called an *ordinary point* of the differential equation. □

With this terminology, we can say that if ξ is an ordinary point of a differential equation, the solution space in $C[[x - \xi]]$ has dimension r. This follows from Theorem 3.1 after applying the change of variables $x' = x + \xi$ to the equation. This change of variables moves the point ξ of interest to the origin. Another change of variables which is sometimes useful is to set $x' = 1/x$. Informally, this substitution moves the "point at infinity" to the origin. More precisely, a solution in $C[[x']]$ of the transformed equation corresponds to a solution of the original equation which belongs to the ring $C[[x^{-1}]]$ of formal power series with descending powers. Such series can be used for describing the asymptotic behaviour of a function as the argument tends to infinity. We will extend the terminology of the previous definition to the "point at infinity" in this sense: ∞ is a singularity of a differential equation if and only if 0 is a singularity of the differential equation obtained by applying the change of variables $x' = 1/x$.

Example 3.15 The differential equation

$$(x - 1)x(2x - 1)(2x + 1)f''(x) + 2(4x^3 - 2x + 1)f'(x) - 2f(x) = 0$$

has the finite singularities $0, 1, 1/2, -1/2$. If we set $g(x) = f(1/x)$, then the differential equation for f translates into the differential equation

$$(x-2)(x-1)(x+2)g''(x) + 2(x-4)g'(x) - 2g(x) = 0.$$

for g. Since this second equation does not have a singularity at 0, we say that the first equation does not have a singularity at infinity. □

We want to determine the solution space in $C[[x-\xi]]$ of a given differential equation at a given point. We have already seen that the space has dimension r whenever ξ is an ordinary point. The following theorem makes this statement a bit more precise.

Theorem 3.16 *Let* $p_0, \dots, p_r \in C[x]$, $p_r \neq 0$. *Suppose that* $\gcd(p_0, \dots, p_r) = 1$ *and consider the differential equation* $p_0 f + \dots + p_r f^{(r)} = 0$. *Then* 0 *is an ordinary point if and only if the solution space of the differential equation in* $C[[x]]$ *has a basis of the form*

$$\begin{aligned}
&1 + 0x + \dots + 0x^{r-1} + b_{0,r}x^r + b_{0,r+1}x^{r+1} + \cdots,\\
&0 + 1x + \dots + 0x^{r-1} + b_{1,r}x^r + b_{1,r+1}x^{r+1} + \cdots,\\
&\vdots\\
&0 + 0x + \dots + 1x^{r-1} + b_{r-1,r}x^r + b_{r-1,r+1}x^{r+1} + \cdots
\end{aligned}$$

for certain $b_{i,j} \in C$. □

Proof "⇒": Follows from Theorem 3.1.

"⇐": Suppose there is a basis of the announced form, and write the basis elements as $b_k := x^k + b_{k,r}x^r + \cdots$ $(k = 0, \dots, r-1)$. We have $p_0 b_k + \dots + p_r b_k^{(r)} = 0$ for $k = 0, \dots, r-1$. In particular, the coefficient of x^0 of $p_0 b_k + \dots + p_r b_k^{(r)}$ is zero for every k. Because of $b_k^{(i)} = k^{\underline{i}} x^{k-i} + b_{k,r} r^{\underline{i}} x^{r-i} + \cdots$ $(k = 0, \dots, r-1,$ $i = 0, \dots, r)$, we have

$$0 = [x^0] \sum_{i=0}^{r} p_i b_k^{(i)} = ([x^0]p_k)k! + ([x^0]p_r) b_{k,r} r!$$

for $k = 0, \dots, r-1$.

In order to show that 0 is an ordinary point, assume it is not. Then $x \mid p_r$, which means $[x^0]p_r = 0$. But then $([x^0]p_k)k! = 0$ for $k = 0, \dots, r-1$, so $x \mid p_k$ for all k. This is impossible because of the assumption that $\gcd(p_0, \dots, p_r) = 1$. ■

As we have seen in Example 3.13, an equation of order r may also have a solution space of dimension r at a singularity. If this happens, we call the singularity apparent.

Definition 3.17 Let $p_0, \dots, p_r \in C[x]$, $p_r \neq 0$. A root ξ of p_r is called an *apparent singularity* of the differential equation $p_0 f + \dots + p_r f^{(r)} = 0$ if the solution space in $C[[x-\xi]]$ of this equation has dimension r.

If infinity is a singularity of the equation, it is called apparent when the solution space in $C[[x^{-1}]]$ has dimension r. □

Using Theorem 3.5, we can determine the basis of the solution space in $C[[x]]$ of a given differential equation. It suffices to translate the differential equation into a recurrence for the coefficient sequence and then use Algorithm 2.13 to find a basis of the solution space of that recurrence. It must be observed however that not every sequence solution in $C^{\mathbb{N}}$ translates into a series solution. A counterexample is given below. Instead, we must take the space of all sequence solutions in $C^{\mathbb{Z}}$ which are zero for the negative integers. To find these, use Algorithm 2.13 to determine a basis of the space of sequence solutions $(a_n)_{n=-r-d}^{\infty} \in C^{-d-r+\mathbb{N}}$ and then determine the subspace of all solutions with $a_{-1} = a_{-2} = \cdots = a_{-d-r} = 0$.

Example 3.18

1. The recurrence equation corresponding to the differential equation

$$(x-1)^2 f''(x) - (x-2)(x-1)f'(x) - f(x) = 0$$

in the sense of Theorem 3.5 is

$$(n+3)(n+2)a_{n+3} - 2(n+2)^2 a_{n+2} + (n^2+4n+2)a_{n+1} - na_n = 0.$$

This recurrence has a solution in $C^{\mathbb{N}}$ which starts like $0, 0, 1, \frac{4}{3}, \frac{17}{12}, \frac{43}{30}, \ldots$. For the corresponding series $f(x) = x^3 + \frac{4}{3}x^4 + \cdots$ we have

$$(x-1)^2 f''(x) - (x-2)(x-1)f'(x) - f(x) = 2 \neq 0,$$

so this series is not a solution of the differential equation.
A basis of the solution space in $C[[x]]$ is given by the two series

$$1 + 0x + \tfrac{1}{2}x^2 + \tfrac{2}{3}x^3 + \tfrac{17}{24}x^4 + \cdots,$$
$$0 + 1x + 1x^2 + 1x^3 + 1x^4 + \cdots.$$

2. The recurrence equation associated to the differential equation $xf'(x) - 5f(x) = 0$ is $(n-5)a_n = 0$, which indicates the solution $f(x) = x^5$.
3. If 0 is an ordinary point of a differential equation of order r and degree d, the leading coefficient polynomial of the associated recurrence is $(n+s)^{\underline{r}}$, where s is the order of the recurrence. This follows directly from Theorem 3.5. To see that the converse is not true, consider the differential equation

$$x(x+1)(x-1)f''(x) + x(x+3)f'(x) - f(x) = 0.$$

The factor x in the leading coefficient indicates that 0 is a singular point. Nevertheless, the associated recurrence,

$$(n + 1)(n + 2)a_{n+2} - (3n + 2)a_{n+1} - n^2 a_n = 0,$$

does have the leading coefficient $(n + 2)^2$.
The singularity is not even apparent, because the potential sequence solution with $a_{-2} = a_{-1} = 0$ and $a_0 = 1$ does not admit a continuation which is consistent with the recurrence (setting $n = -1$ in the recurrence would produce $1 = 0$ regardless of the choice of a_1). The only formal power series solution of the equation (up to constant multiples of course) is the geometric series $x + x^2 + x^3 + \cdots$. □

Not only power series solutions of differential equations are of interest. Depending on the application, we might instead consider the space of all analytic or meromorphic function solutions defined on a certain open subset of $\mathbb{C}$. It can also be of interest to ask for formal solutions, i.e., solutions which can be expressed in "closed form". The latter is made precise using the notion of differential rings.

Definition 3.19 Let R be a commutative ring and let $D: R \to R$ be a map satisfying

$$D(a + b) = D(a) + D(b) \quad \text{and} \quad D(ab) = D(a)b + aD(b)$$

for all $a, b \in R$. Such a map is called a *derivation* on R.

1. The pair (R, D) is called a *differential ring*. If R is a field, it is called a *differential field.*
2. An element $c \in R$ is called a *constant* if $D(c) = 0$. The set of all constants of R is denoted by $\mathrm{Const}(R)$.
3. If (E, Δ) is a differential ring such that R is a subring of E and $\Delta|_R = D$, then (E, Δ) is called a *differential ring extension* of (R, D). If R is a field, (E, Δ) is called a *differential field extension* of (R, D). □

We will take the freedom to simply write R instead of (R, D) when D is clear from the context. Also, for a differential ring extension (E, Δ) of a differential ring (R, D), we will often use the same name for D and Δ. It is easy to show that $\mathrm{Const}(R)$ is always a subring of R; it is called the constant ring of R. Whenever R is a field, $\mathrm{Const}(R)$ is a field, called the constant field of R in this case. In particular, 0 and 1 are always constants.

Examples of differential rings include $C[x]$, $C(x)$, $C[[x]]$, $C((x))$ with the usual derivations as D. They all have C as their constant field. A rational function field $C(x_1, \dots, x_n)$ can be turned into a differential field in many ways. In fact, for any choice $r_1, \dots, r_n \in C(x_1, \dots, x_n)$, there is a unique derivation $D: C(x_1, \dots, x_n) \to C(x_1, \dots, x_n)$ with $D(x_i) = r_i$ for $i = 1, \dots, n$ (Exercise 15). This construction can be used to design differential fields whose elements behave under derivation like certain functions of interest. For example, taking $K = C(x, y, z)$ and setting $D(x) = 1$, $D(y) = y$, and $D(z) = \frac{1}{x}$ turns K

into a differential field in which x behaves like a variable, y behaves like the function $\exp(x)$, and z behaves like the function $\log(x)$.

We will usually assume that the field $C(x)$ is equipped with the usual derivation (i.e., $D(x) = 1$). If K is any differential field extension of $C(x)$, then it is meaningful to ask for solutions in K of a linear differential equation with coefficients $p_0, \ldots, p_r \in C(x)$: these are the elements $y \in K$ for which we have

$$p_0 y + p_1 D(y) + \cdots + p_r D^r(y) = 0.$$

These solutions form a vector space of dimension at most r, as we show next.

Theorem 3.20 *(See Theorem 2.26 for the shift case) Let (K, D) be a differential field, and let $p_0, \ldots, p_r \in K$ with $p_r \neq 0$. Let*

$$V = \{ y \in K : p_0 y + p_1 D(y) + \cdots + p_r D^r(y) = 0 \} \subseteq K.$$

Then V is a vector space over Const(K) *of dimension at most r.* □

Proof It is easy to check that V is a vector space over Const(K). To show the bound on the dimension, let $y_0, \ldots, y_r \in V$. We show that they are linearly dependent over Const(K).

The case $r = 1$ is settled in Exercise 8. Suppose that $r > 1$. The vectors

$$Y_i = (y_i, D(y_i), \ldots, D^{r-1}(y_i)) \in K^r$$

are linearly dependent over K, because $r + 1$ elements of K^r are always linearly dependent over K.

Let $c_0, \ldots, c_r \in K$, not all zero, be such that $\sum_{i=0}^r c_i Y_i = 0$. Then in particular $\sum_{i=0}^r c_i y_i = 0$ and since $r > 1$, $\sum_{i=0}^r c_i D(y_i) = 0$. We may assume that among all possible choices for the c_i, we have chosen one such that $c_{k+1} = \cdots = c_r = 0$ for the smallest possible $k \in \{0, \ldots, r\}$. We may further assume that $c_k = 1$ (otherwise replace each c_i by c_i/c_k).

Now $\sum_{i=0}^r c_i y_i = 0$ implies

$$0 = D(\sum_{i=0}^r c_i y_i) = \sum_{i=0}^r D(c_i) y_i + \sum_{i=0}^r c_i D(y_i).$$

By the assumption $r > 1$, and by the choice of c_i, the last sum is zero. Furthermore, because of $D(c_k) = D(1) = 0$, the other sum on the right hand side is equal to $\sum_{i=0}^{k-1} D(c_i) y_i$. By the minimality of k, it follows that $D(c_0) = \cdots = D(c_{k-1}) = 0$, so $c_0, \ldots, c_{k-1}, c_k, c_{k+1}, \ldots, c_r \in$ Const(K), as claimed. ■

If K is just an integral domain, we can extend a derivation defined on K to a derivation of its quotient field Quot(K). If this does not lead to new constants, i.e., if Const(K) = Const(Quot(K)), then the theorem can also be applied to K. In particular, the solution space in $C[[x]]$ of a differential equation of order r with coefficients in $C[x]$ has dimension at most r. This is consistent with the result of Theorem 3.20, where we have seen that the coefficient sequence of a power series solution satisfies a recurrence with polynomial coefficients of degree at most r, which implies that there are at most r candidates for the starting exponents of a power series solution.

It is important to note that Theorem 3.20 only makes a statement about the dimension of V as a vector space over $\operatorname{Const}(K)$. Depending on the choice of K, the constant field may be larger than expected. For example, consider the differential field $K = C(x, y)$ with $D(c) = 0$ for $c \in C$, $D(x) = x$, and $D(y) = -2y$. By construction, C is contained in the constant field of K, but there are further elements: $D(yx^2) = D(y)x^2 + yD(x)x + yxD(x) = -2yx^2 + yx^2 + yx^2 = 0$ shows that $yx^2 \in \operatorname{Const}(K)$, although $yx^2 \notin C$. We call constants in $\operatorname{Const}(K) \setminus C$ *fake constants,* because they usually cause confusion.

We can view the generators x, y in this example as formalizations of the functions $\exp(t)$ and $\exp(-2t)$, because $\exp'(t) = \exp(t)$ and $\exp'(-2t) = -2\exp(-2t)$. Doing so, it is not surprising that $\exp(t)^2 \exp(-2t) = 1$ turns out to be a constant. Informally speaking, the differential field K recognizes that yx^2 is the formalization of a constant function, but it does not know the value of this function. This is because the specification $D(x) = x$ is compatible not just with the interpretation $x = \exp(t)$, but also with $x = 5\exp(t)$, for example.

If we have a particular interpretation in mind, the construction of the differential field should reflect this information by imposing suitable algebraic relations among the generators. For example, if x and y are meant to represent $\exp(t)$ and $\exp(-2t)$, respectively, it suffices to consider the differential field $C(x)$ with $D(x) = x$, and use $1/x^2$ instead of a separate variable y.

Theorem 3.20 provides an upper bound for the dimension of the solution space. In general, this bound is not reached. However, it is always reached for K sufficiently large, in the sense that every linear differential equation of order r with coefficients in K has r linearly independent solutions in a certain differential field extension E of K. Our next goal is to make this statement precise. We will construct E by first imposing a differential ring structure on a polynomial ring over K, then taking the quotient by a suitable ideal of relations (to get rid of fake constants), and finally taking the fraction field. In order to make the first step work, we need to ensure that the differential ring structure can be carried over to the quotient ring. In order to make the second step work, we need to ensure that the quotient ring is an integral domain. The following lemma provides the required facts.

Lemma 3.21 *Let R be a ring of characteristic zero and D be a derivation on R.*

1. *If I is an ideal of R which is closed under D, i.e., $\forall\, a \in I : D(a) \in I$, then the ring $\bar{R} := R/I$ together with $\bar{D}\colon \bar{R} \to \bar{R}$, $\bar{D}(a+I) := D(a)+I$ is a differential ring.*
2. *If the only ideals of R which are closed under D are $\{0\}$ and R, then R is an integral domain.*

3. *If R is an integral domain, then the derivation D can be uniquely extended to a derivation on the quotient field* $\mathrm{Quot}(R)$.
4. *If the only ideals of R which are closed under D are* $\{0\}$ *and R, then* $\mathrm{Const}(\mathrm{Quot}(R)) \subseteq R$.

Proof

1. If $u = v \bmod I$, then $u - v \in I$, then $D(u - v) = D(u) - D(v) \in I$, then $D(u) = D(v) \bmod I$, as required.
2. Let $a, b \in R$ be such that $a \neq 0$ and $ab = 0$. We have to show that $b = 0$.
   Assume first that a is not nilpotent, i.e., $a^n \neq 0$ for all $n \in \mathbb{N}$. We have $b \in J := \{u \in R \mid \exists\, n : a^n u = 0\}$. We show that $J = \{0\}$. This follows from the assumption because J is a proper ideal of R (note that $1 \notin J$ because a is not nilpotent), and because J is closed under D (as shown in Exercise 16).
   We have thus shown that all zero divisors must be nilpotent. Now let J be the set of all nilpotent elements of R. Again, this is a proper ideal of R (clearly, at least 1 is not nilpotent), and it is closed under D, because if u is nilpotent and $n \in \mathbb{N}$ is minimal with $u^n = 0$, then $u^n = 0 \Rightarrow D(u^n) = nu^{n-1}D(u) = 0$, so $D(u)$ is a zero divisor (because $n > 0$ and $u^{n-1} \neq 0$), so $D(u)$ must be nilpotent as well. By the assumption, it follows that $J = \{0\}$, so R does not have any nilpotent elements.
3. For $z = p/q \in \mathrm{Quot}(R)$ we have $zq - p = 0$, so we must have $0 = D(zq - p) = D(z)q + zD(q) - D(p)$, i.e., $D(z) = (D(p) - zD(q))/q = (D(p)q - pD(q))/q^2$, the usual quotient rule.
4. Let $a \in \mathrm{Const}(\mathrm{Quot}(R))$. The ideal $I = \{b \in R : ab \in R\}$ is closed under D, because for every $b \in I$ we have $D(ab) = D(a)b + aD(b) = aD(b)$, so $D(b) \in I$. Since I is not the zero ideal (it contains at least the denominator of a), it follows from the assumption that $I = R$. Then $1 \in I$ implies $a \in R$. ■

An ideal of a differential ring R which is closed under D is called a *differential ideal.*

Let K be a differential field and consider a differential equation $p_0 y + \cdots + p_r D^r(y) = 0$ with $p_0, \ldots, p_r \in K$ and $p_r \neq 0$. A differential ring containing a solution of this equation is easily constructed by taking the polynomial ring $R = K[y_0, \ldots, y_{r-1}]$ in r new variables and extending D to R via $D(y_j) = y_{j+1}$ ($j = 0, \ldots, r-1$) and $D(y_{r-1}) = -\frac{1}{p_r}(p_0 y_0 + p_1 y_1 + \cdots + p_{r-1} y_{r-1})$. This turns R into a differential ring in which y_0 is a solution of the differential equation.

If we want to have several solutions, we can use several sets of r variables, i.e., set

$$R = K[y_{1,0}, \ldots, y_{1,r-1}, \ldots\ldots, y_{r,0}, \ldots, y_{r,r-1}]$$

and define $D\colon R \to R$ by $D(y_{i,j}) = y_{i,j+1}$ ($i = 1, \ldots, r$, $j = 0, \ldots, r-1$) and $D(y_{i,r-1}) = -\frac{1}{p_r}(p_0 y_{i,0} + p_1 y_{i,1} + \cdots + p_{r-1} y_{i,r-1})$ ($i = 1, \ldots, r$). Then $y_{1,0}, \ldots, y_{1,r}$ are solutions of the differential equation. Being variables of a polynomial ring, the $y_{i,j}$ are not only linearly independent over C but even algebraically independent over K. However, the ring R will in general have fake constants.

In order to get rid of possible fake constants, we will consider R/M for some differential ideal M. The ideal should be large enough to ensure that R/M has no nontrivial differential ideals, so that Lemma 3.21 ensures that R/M is an integral domain. On the other hand, M should not be too large, because if it contains elements like $y_{1,0}-y_{3,0}$, this would destroy the linear independence of the solutions. We can preserve the linear independence by adding one additional variable z to the ring and forcing the ideal to contain the polynomial $z\det(y_{i,j})-1$, where $\det(y_{i,j}) \in R$ refers to the determinant of the matrix $((y_{i,j}))_{i=1,j=0}^{r,r-1} \in R^{r\times r}$. In view of Exercise 9, we can (and must) extend D to $R[z]$ by setting $D(z) = -z^2 D(\det(y_{i,j}))$. Also note that $c_1 y_{1,0} + \cdots + c_r y_{r,0} = 0$ implies $c_1 D^j(y_{1,0}) + \cdots + c_r D^j(y_{r,0}) = 0$ for every j, so by forcing the columns of $((y_{i,j}))_{i=1,j=0}^{r,r-1} \in R^{r\times r}$ to be linearly independent over K, we in particular force the $y_{i,0}$ to be linearly independent over C.

Thus, let $I = \langle z\det(y_{i,j}) - 1\rangle \subseteq R[z]$. Among all of the differential ideals $J \subsetneq R[z]$ with $I \subseteq J$, there must be some which are maximal with respect to inclusion. This follows from the ascending chain condition for polynomial rings (see, e.g., Sect. 1.4 of [184] or Thm. 7 in Sect. 2§5 of [167]). Let M be such a maximal ideal and set $\bar{R} := R[z]/M$. The maximality ensures that the only differential ideals of $\bar{R}$ are $\{0\}$ and $\bar{R}$, so Lemma 3.21 ensures that $\bar{R}$ is an integral domain. We can therefore take the quotient field $E = \mathrm{Quot}(\bar{R})$. By construction, this field contains r linearly independent solutions of the differential equation. Using a result from algebraic geometry, we can also show that it does not have any fake constants.

Theorem 3.22 *Let K be a differential field with an algebraically closed field C of constants. Let $p_0, \ldots, p_r \in K$, $p_r \neq 0$. Then there exists a differential field extension E of K with* $\mathrm{Const}(E) = C$ *such that the solution space*

$$\{\, y \in E : p_0 y + \cdots + p_r D^r(y) = 0 \,\}$$

has dimension r over C. □

Proof Define the field $E = \mathrm{Quot}(\bar{R})$ as described above. It follows from the previous discussion that E contains r solutions of the differential equation which are linearly independent over $\mathrm{Const}(E)$. It remains to show that $\mathrm{Const}(E) = C$. It is clear that C is contained in $\mathrm{Const}(E)$. To show the opposite inclusion, suppose there is an $a \in \mathrm{Const}(E) \setminus C$. We will show that a is algebraic over C, thereby obtaining a contradiction to the assumption that C is algebraically closed.

According to Lemma 3.21, $a \in \mathrm{Const}(\mathrm{Quot}(\bar{R})) \setminus C$ implies $a \in \mathrm{Const}(\bar{R}) \setminus C$. Therefore, $\langle a - c\rangle$ is a nonzero differential ideal for every $c \in C$. This implies $1 \in \langle a - c\rangle$ for every $c \in C$, i.e., $a - c$ is invertible in $\bar{R}$ for every $c \in C$.

Recall that R is a polynomial ring over K in r^2 variables, and that $\bar{R} = R[z]/M$ for a certain ideal M, with z an additional variable. Let $\bar{K}$ be the algebraic closure of K and let $X \subseteq \bar{K}^{r^2+1}$ be the zero set of M. We can view $a \in \bar{R}$ as a polynomial map $X \to \bar{K}$. By a result from algebraic geometry (Chevalley's theorem, see, e.g., Cor. 14.7 of [184]), we must have either $|\operatorname{im} a| < \infty$ or $|\bar{K} \setminus \operatorname{im} a| < \infty$. Since $a-c$ is invertible in $\bar{R}$ for every $c \in C$, we have $\operatorname{im} a \cap C = \emptyset$, so $C \subseteq \bar{K} \setminus \operatorname{im} a$, so $|\bar{K} \setminus \operatorname{im} a| = \infty$, so $|\operatorname{im} a| < \infty$.

From $|\operatorname{im} a| < \infty$ it follows that a is algebraic over K, for if $\operatorname{im} a = \{u_1, \dots, u_m\}$ for certain $u_1, \dots, u_m \in \bar{K}$, and if $u_i^{(1)}, \dots, u_i^{(\ell_i)} \in \bar{K}$ are the conjugates of u_i for every i, then we have $\prod_{i=1}^m \prod_{j=1}^{\ell_i} (a - u_i^{(j)}) = 0$ in $\bar{R}$, showing that a is a root of a polynomial with coefficients in K.

Let $q = q_0 + q_1 x + \cdots + q_d x^d \in K[x]$ be such a polynomial. We may assume that d is minimal and $q_d = 1$. Then

$$0 = D(q(a)) = D(q_0) + D(q_1)a + \cdots + \underbrace{D(q_d)}_{=0} a^d + \underbrace{q_1 D(a) + \cdots + q_d d a^{d-1} D(a)}_{=0,\text{ because } a \text{ is a constant}}.$$

By the minimality of d, it follows that $D(q_0) = \cdots = D(q_{d-1}) = 0$, so $q_0, \dots, q_{d-1} \in \operatorname{Const}(K) = C$, so a is algebraic over C, so $a \in C$. ■

In a sense, the field $E = \operatorname{Quot}(\bar{R})$ is the smallest differential field containing K and a full set of r linearly independent solutions of the equation $p_0 y + \cdots + p_r D^r(y) = 0$. It can be shown that it is unique up to (differential) isomorphism (cf., e.g., Proposition 1.20 in [441]). The field is called the *Picard-Vessiot-extension* of K for the equation. It is the differential analog of the splitting field of a polynomial known from classical algebra.

Example 3.23 Let $K = C(x)$ be equipped with the usual derivation, and consider the differential equation

$$(x-1)y + (1-2x)y' + xy'' = 0.$$

It has the two linearly independent solutions $\exp(x)$ and $\exp(x)\log(x)$. We want to construct the Picard-Vessiot-field for this equation.

First, set $R = K[y_{1,0}, y_{1,1}, y_{2,0}, y_{2,1}, z]$ and extend the derivation on K to R by setting $D(y_{i,0}) = y_{i,1}$ and $D(y_{i,1}) = -\frac{x-1}{x} y_{i,0} - \frac{1-2x}{x} y_{i,1}$ for $i = 1, 2$, and $D(z) = -z^2(y_{1,0}y_{2,1} - y_{2,0}y_{1,1})$. Then $y_{1,0}$ and $y_{2,0}$ are two linearly independent solutions. Being variables of a polynomial ring, they are even algebraically independent over K.

Since we already know the solutions, we can imagine $y_{1,0}$ and $y_{2,0}$ as being certain C-linear combinations of $\exp(x)$ and $\exp(x)\log(x)$. Then, since

$$D(\alpha \exp(x) + \beta \exp(x)\log(x)) = \alpha \exp(x) + \beta \exp(x) + \beta \exp(x)/x,$$

for any choice $\alpha, \beta \in C$, we notice that $y_{1,0} - y_{1,1}$ and $y_{2,0} - y_{2,1}$ must behave like constant multiples of $\exp(x)/x$. This suggests that their quotient might be a constant.

Indeed, in $\mathrm{Quot}(R)$, we formally have $D(\frac{y_{1,0}-y_{1,1}}{y_{2,0}-y_{2,1}}) = 0$ as a consequence of how D is defined on R. We can eliminate this constant by identifying it with some element of C. It turns out that for any $\gamma \in C$ we can take $J = \langle (y_{1,0}y_{2,1} - y_{2,0}y_{1,1})z - 1, (y_{1,0} - y_{1,1}) - \gamma(y_{2,0} - y_{2,1})\rangle$, and R/J will not have any fake constants.

But we are not done yet, because R/J has nontrivial differential ideals. Again, knowing the solutions explicitly helps to see where they come from. Since $y_{1,0}$ and $y_{2,0}$ can be regarded as certain C-linear combinations of $\exp(x)$ and $\exp(x)\log(x)$, there should be some C-linear combination of them which behaves like $\exp(x)$. Since we already noticed that $y_{2,0} - y_{2,1}$ must behave like $\exp(x)/x$, this suggests an additional relation of the form $\alpha y_{1,0} + \beta y_{2,0} = x(y_{2,0} - y_{2,1})$ for some $\alpha, \beta \in C$. This relation does not lead to a fake constant because its coefficients depend not only on the differential equation but also on the choice of the particular linear combination of $\exp(x)$ and $\exp(x)\log(x)$ to which $y_{1,0}$ and $y_{2,0}$ correspond. This choice is essentially up to us.

If we let $y_{1,0}$ play the role of $\exp(x)$ and $y_{2,0}$ play the role of $\exp(x)\log(x)$, then we have $\alpha = 1$, $\beta = 0$, $\gamma = 0$. This choice leads to the differential ideal

$$M = \langle (y_{1,0}y_{2,1} - y_{2,0}y_{1,1})z - 1, y_{1,0} - y_{1,1}, y_{1,0} - x(y_{2,0} - y_{2,1})\rangle \subseteq R,$$

which turns out to be maximal.

With this choice, the Picard-Vessiot field is $E = \mathrm{Quot}(R/M)$. All other possible choices of α, β, γ amount to writing the same field in terms of other generators. Note that E is isomorphic to the differential field $C(x, \exp(x), \log(x))$. □

Although it is appropriate for most applications to think of the solutions of a given differential equation as elements of a certain differential ring, we do have the possibility to allow further generality. Consider, as before, a linear differential equation $p_0 y + \cdots + p_r D^r(y) = 0$ with coefficients in a certain differential ring R, e.g., $R = C[x]$. In order to make it meaningful to ask for solutions of this equation in some universe U, it is sufficient to require that there is a certain extension of D to U, so that we can "differentiate" elements of U, and that U is an R-module, so that it is meaningful to take R-linear combinations of an element y of U and its derivatives.

In this setting, it might not be possible to multiply elements of U with each other, but we only assume that it is possible to multiply elements of R with elements of U. The extension of the derivation $D\colon R \to R$ to a map $D\colon U \to U$ must be such that the product rule continues to hold for these multiplications. Of course, D must also continue to be additive, so altogether we require that $D(u + v) = D(u) + D(v)$ and $D(pu) = D(p)u + pD(u)$ for all $u, v \in U$ and all $p \in R$. An R-module U together with such a D is called a *D-module* (over R).

If R is a differential field and U is a D-module (over K), then an element $u \in U$ is called D-finite if the K-vector space generated by $u, D(u), D^2(u), \ldots$ over K in U has finite dimension. Equivalently, u is D-finite if there are $p_0, \ldots, p_r \in K$, not all zero, such that $p_0 u + \cdots + p_r D^r(u) = 0$.

Example 3.24

1. Any differential ring extension E of R is a D-module in a natural way.
2. Let $R = C[x]$ and U be the set of all bilateral infinite series $\sum_{n=-\infty}^{\infty} a_n x^n$ with coefficients in C. Then there is no natural way to turn U into a ring, but U is still a D-module over R.
   Note that while it is fair to clear common factors from a differential equation if we are looking for solutions in an integral domain, we must be more careful when solutions are sought in a D-module. To see why, observe that the equation $(1-x)y = 0$ (a differential equation of order 0) has the nonzero solution $\sum_{n=-\infty}^{\infty} x^n$ in U, while the equation $y = 0$ obviously has no nonzero solution.
3. Let R be a differential ring and E be a differential ring extension of R. Let $f \in E$ and $F \subseteq E$ be the set of all R-linear combinations of $f, D(f), D^2(f), \ldots$. Then F is a D-module, but in general not a subring of E.
   To be more specific, take $R = C(x)$, $E = C(x, \exp(x))$, and $F = C(x)\exp(x)$. Then F consists of all $C(x)$-linear combinations of $\exp(x)$ and its derivatives. Note that E contains $\exp(x)^2$ but F does not. □

Exercises

1**.** Consider a differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ for some $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$. Let $a_{i,j} = \delta_{i,j}$ if $i = 0$ or $j = 0$ and $a_{i,j} = \binom{j}{i}\frac{(j-1)!}{(i-1)!}$ for $i, j > 0$. Show that for $g(x) = f(1/x)$ we have the differential equation $q_0(x)g(x) + \cdots + q_r(x)g^{(r)}(x) = 0$ with $q_i(x) = \sum_{j=i}^{r} p_j(1/x)(-1)^j a_{i,j} x^{i+j}$ for $i = 0, \ldots, r$.

Hint: First show that $f^{(i)}(x) = (-1)^i \sum_{j=0}^{i} a_{j,i} g^{(j)}(1/x) x^{-(i+j)}$ for $i = 0, \ldots, r$.

2. Find a basis of the solution space of $(3x^5 + x^2)f''(x) + (-18x^4 + 4x^2 - 3x)f'(x) + (30x^3 + 4x^2 - 6x + 4)f(x) = 0$ in $\mathbb{Q}[[x]]$.

3. Find a basis of the solution space of $4x^2(3x^3 + 1)(x + 1)^2 f''(x) + 4x(4x + 5)(x + 1)f'(x) + (9x^2 + 22x + 16)f(x) = 0$ in $\mathbb{Q}((x))$.

4. Find a basis of the solution space of $x(x^4 - 4x^2 + 5)f''(x) + (8x^4 - 33x^2 + 39)f'(x) + 10(x - 2)x(x + 2)f(x) = 0$ in $\mathbb{Q}[[x^{-1}]]$.

5. Construct a differential equation whose solution space in $\mathbb{C}[[x]]$ has a larger dimension than its solution space in the field $\mathfrak{M}$ of meromorphic functions defined in a neighborhood of zero.

6*. Show that the dimension of the solution space of a differential equation of order r in a differential field K can be any number in $\{0, \ldots, r\}$.

Hint: Show first that for every choice of $\alpha_1, \ldots, \alpha_r \in C$ there is a differential equation of order r with coefficients in $C(x)$ whose solution space is generated by

$x^{\alpha_1}, \ldots, x^{\alpha_r}$. Taking $K = C(x)$ and choosing d integral and $r - d$ non-integral α's shows the claim.

7. Show that $\sqrt{\sin(x)}$ is not D-finite.

8. Show Theorem 3.20 for the case $r \leq 1$.

9. Let K be a differential field, $a, b \in K \setminus \{0\}$, and $n, m \in \mathbb{Z}$.

a. Show that $D(1/a) = -D(a)/a^2$.

b. Show that $D(a^n) = na^{n-1}D(a)$.

c. Show that $D(a^n b^m)/(a^n b^m) = nD(a)/a + mD(b)/b$.

10. Let (R, D) be a differential ring, let $u \in R$ and $p \in R[x]$. Show that $D(p(u)) = p'(u)D(u) + \delta_D(p)(u)$, where p' is the usual derivative of p (i.e., $(a_0 + a_1x + a_2x^2 + \cdots)' = (a_1 + 2a_2x + \cdots))$ and $\delta_D(p)$ is the polynomial obtained from p by applying D to its coefficients (i.e., $\delta_D(a_0 + a_1x + \cdots) = D(a_0) + D(a_1)x + \cdots$).

11*. Determine the constants of the differential rings $C(x)$ and $C[[x]]$ with the derivation defined by $D(x) = 1$.

12. What are the constants of the differential field $C(x, y)$ with $D(x) = D(y) = 1$?

13. Let K be a differential field with $\mathbb{Q} \subseteq K$. Show that $\mathbb{Q} \subseteq \operatorname{Const}(K)$.

14. Prove or disprove: $D\colon C[x] \to C[x]$, $D(f) = -f''$ is a derivation.

15. Let (R, D) be a differential ring and $u \in R$. Show that there is a unique extension of D to a derivation on $R[x]$ such that $D(x) = u$.

16. Show that the ideal J in the proof of part 2 of Lemma 3.21 is indeed closed under D.

17*. Let (K, D) be a differential field and $u \in K[x]$ irreducible. Show that there is a unique extension of D to a derivation on the algebraic extension $K[x]/\langle u \rangle$.

18. Consider a linear differential equation $p_0 y + \cdots + p_r D^r(y) = 0$ with constant coefficients $p_0, \ldots, p_r \in C$.

a. Show that every root $\xi \in C$ of the polynomial $p_0 + \cdots + p_r x^r$ gives rise to a solution $\exp(\xi x)$.

b. Find the Picard-Vessiot extension of C for the equation $14y + 32y' - 7y'' - 6y''' + y^{(4)} = 0$.

19. Let R_1, R_2 be two differential rings containing $C[x]$, and let $\phi\colon R_1 \to R_2$ be a ring homomorphism that respects differentiation and leaves $C[x]$ fixed, i.e., $\phi(D(u)) = D(\phi(u))$ for all $u \in R_1$ and $\phi(u) = u$ for all $u \in C[x]$. Consider a differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ with $p_0, \ldots, p_r \in C[x]$. Show that whenever $y \in R_1$ is a solution of this equation, then so is $\phi(y) \in R_2$.

20. Where in the proof of Lemma 3.21 did we use the assumption that R has characteristic zero?

21. Find a basis for the solution space of the differential equation $(x-1)y'+xy = 0$ in the D-module U consisting of all bilateral infinite series $\sum_{n=-\infty}^{\infty} a_n x^n$.

22⋆. Find a basis for the solution space of the differential equation $y-y' = 0$ in the D-module U consisting of all meromorphic functions defined on $B_{-2}(1) \cup B_2(1) \subseteq \mathbb{C}$ (the union of the unit discs with centers at -2 and $+2$, respectively).

23. Let (K, D) be a differential field and let u, v be nonzero elements of K. Consider the differential field extension $E = K(y_1, y_2, y_3)$ with $D(y_1) = D(u)/u$, $D(y_2) = D(v)/v$, and $D(y_3) = D(uv)/(uv)$, so that y_1, y_2, y_3 can be understood as $\log(u)$, $\log(v)$, $\log(uv)$, respectively. Show that E has fake constants.

References

Besides the important feature that their solution set forms a vector space, another important feature of linear differential equations with polynomial coefficients is that their solutions can have singularities at finitely many positions only. This is a key difference to nonlinear differential equations. For example, observe that the nonlinear equation $f'(x) - f(x)^2 = 0$ has the solution $f(x) = 1/(x-c)$ for arbitrary $c \in C$, so there is no point in C where all solutions of the equation can be described by power series.

Schlesinger remarks in the preface to his handbook [381] that these two features of linear differential equations were a key motivation for the development of the theory. Indeed, as we will also see in more detail in the rest of this chapter, singularities are a valuable source of information about the solutions of a differential equation.

The algebraic view to the theory of differential equations forms the field of *differential algebra*. It was introduced by Ritt [371] in 1950; another classical reference is the book of Kaplansky [257]. This theory is fairly general and also offers an algebraic perspective to nonlinear equations. The case of linear equations is the focus of the book of van der Put and Singer [441] on Galois theory for Picard-Vessiot extensions. Our discussion of Theorems 3.20 and 3.22 follows this book.

3.3 Closure Properties

In the previous section we were concerned with the set of all formal power series satisfying a certain given linear differential equation with polynomial coefficients. We found that for any fixed equation, this set is a C-vector space of finite dimension. We now turn to the set all formal power series and want to collect operations on this set which preserve D-finiteness. Such operations are called closure properties. Closure properties are useful for recognizing that a function given in terms of an expression is D-finite. This is evidently the case if all of the innermost subexpressions are D-finite and the expression is built up entirely from operations which preserve D-finiteness. Closure properties are also useful for proving identities among given D-finite functions: in order to prove $f = g$ for two D-finite power series f, g, it suffices to compute a differential equation for the difference $f - g$ and then prove, using the criteria discussed in the previous section, that this series is zero.

Theorem 3.25 *(See Theorem 2.30 for the shift case) Let $f \in C[[x]]$ be D-finite of order r_f and degree d_f and let $g \in C[[x]]$ be D-finite of order r_g and degree d_g.*

1. *$f + g$ is D-finite of order (at most) $r_f + r_g$ and degree (at most) $(r_f + 1)d_g + (r_g + 1)d_f$.*
2. *fg is D-finite of order (at most) $r_f r_g$ and degree (at most) $r_f r_g((r_f(r_g-1) + 1) d_f + (r_g(r_f - 1) + 1)d_g)$.* □

Proof Let $p_i, q_i \in C[x]$ be such that

$$p_0 f + p_1 f' + \cdots + p_{r_f} f^{(r_f)} = 0,$$
$$q_0 g + q_1 g' + \cdots + q_{r_g} g^{(r_g)} = 0.$$

Suppose that p_{r_f} and q_{r_g} are not zero.

1. We can create other differential equations for f and g by differentiating the given equations, or by multiplying them with polynomials, or by adding some of the equations obtained in this way. We will show that there is a differential equation of the announced shape which can be reached via these operations both from the equation given for f and the equation given for g. This equation will therefore have both f and g as solutions, and therefore also their sum $f + g$.
   Make an ansatz

$$\sum_{j=0}^{r_g} u_j D^j (p_0 f + p_1 f' + \cdots + p_{r_f} f^{(r_f)}) = 0,$$
$$\sum_{j=0}^{r_f} v_j D^j (q_0 g + q_1 g' + \cdots + q_{r_g} g^{(r_g)}) = 0,$$

   with unknown polynomial coefficients u_j, v_j. Note that as soon as one u_j is nonzero, the first equation is nontrivial, and likewise for the second.
   Equating the coefficient of $f^{(k)}$ to the coefficient of $g^{(k)}$, for $k = 0, \ldots, r_f + r_g$ gives a linear system with $(r_f + 1) + (r_g + 1)$ variables (the u_j and v_j) and $r_f + r_g + 1$ equations (one for each k). Since the action of D^j cannot increase the degrees of the polynomial coefficients, it follows that the coefficients of the variables u_j are polynomials of degree at most d_f while those of the variables v_j are polynomials of degree at most d_g.

This linear system must have a nonzero solution. By Theorem 1.29, there is a solution vector with polynomial entries where the entries corresponding to the variables u_j have degrees bounded by $r_g d_f + (r_f + 1)d_g$ and those corresponding to the variables v_j have degrees bounded by $(r_g + 1)d_f + r_f d_g$.
Taking as u_j and v_j the components of a solution vector, the equations from the ansatz become equal. Furthermore, for a nonzero solution vector, at least one u_j or one v_j must be nonzero, which forces that at least one of the equations is nontrivial (and then, since the equations are equal, both are nontrivial). Taking also the degrees of p_i and q_i into account, we see that the resulting equations have coefficients of the claimed degree.

2. By differentiating the given equation involving f several times, we obtain equations of the form $p_{r_f} f^{(i)} = \dots$, where the right hand side is a $C[x]$-linear combination of $f, f', \dots, f^{(i-1)}$ with coefficients of degree at most d_f. These equations allow us to rewrite any term $p_{r_f}^{i+1} f^{(r_f+i)}$ with $i \in \mathbb{N}$ as a $C[x]$-linear combination of $f, f', \dots, f^{(r_f-1)}$ with coefficients of degree at most $(i + 1)d_f$. Likewise, for all $i \in \mathbb{N}$ we can write $q_{r_g}^{i+1} g^{(r_g+i)}$ as a $C[x]$-linear combination of $g, \dots, g^{(r_g-1)}$ with coefficients of degree at most $(i + 1)d_g$.
Make an ansatz with undetermined coefficients $u_0, \dots, u_{r_f r_g} \in C[x]$ for a differential equation

$$u_0(fg) + u_1(fg)' + \cdots + u_{r_f r_g} D^{r_f r_g}(fg) = 0.$$

Using the product rule, this equation can be written as a $C[x]$-linear combination of terms of the form $f^{(i)} g^{(j)}$ with $i + j \le r_f r_g$. After multiplying the equation by $p_{r_f}^{r_f r_g - r_f} q_{r_g}^{r_f r_g - r_g}$ we rewrite it as a $C[x]$-linear combination of terms $f^{(i)} g^{(j)}$ with $0 \le i < r_f$ and $0 \le j < r_g$ and coefficients of degrees at most $(r_f(r_g - 1) + 1)d_f + (r_g(r_f - 1) + 1)d_g$ which still depend linearly on the unknown coefficients $u_0, \dots, u_{r_f r_g}$. Equating these coefficients to zero gives a linear system over $C[x]$ with $r_f r_g + 1$ variables (the unknowns u_i) and $r_f r_g$ equations (one for each $f^{(i)} g^{(j)}$).
This linear system must have a nonzero solution. By Theorem 1.29, there is a solution vector with polynomial entries of degree at most $r_f r_g((r_f(r_g - 1) + 1)d_f + (r_g(r_f - 1) + 1)d_g)$. This solution vector gives rise to the desired differential equation for the product fg. ■

Example 3.26 Let $f, g \in C[[x]]$ be power series satisfying the differential equations

$$(x+1)f'' + (2x+1)f' + (x-1)f = 0, \quad (x+2)g'' + (x+1)g' + (2x+3)g = 0.$$

1. Make an ansatz

$$\sum_{j=0}^{2} u_j D^j((x+1)f'' + (2x+1)f' + (x-1)f) = 0,$$
$$\sum_{j=0}^{2} v_j D^j((x+2)g'' + (x+1)g' + (2x+3)g) = 0,$$

for undetermined $u_0, u_1, u_2, v_0, v_1, v_2$. By expanding the derivations and rearranging the terms, the ansatz turns into

$$\begin{aligned}
&u_2(x+1)f^{(4)} + (u_1x + 2u_2x + u_1 + 3u_2)f^{(3)}\\
&\quad + (u_0x + 2u_1x + u_2x + u_0 + 2u_1 + 3u_2)f''\\
&\quad + (2u_0x + u_1x + u_0 + u_1 + 2u_2)f' + (u_0x - u_0 + u_1)f = 0,\\
&v_2(x+2)g^{(4)} + (v_1x + v_2x + 2v_1 + 3v_2)g^{(3)}\\
&\quad + (v_0x + v_1x + 2v_2x + 2v_0 + 2v_1 + 5v_2)g''\\
&\quad + (v_0x + 2v_1x + v_0 + 4v_1 + 4v_2)g' + (2v_0x + 3v_0 + 2v_1)g = 0.
\end{aligned}$$

Equating the coefficients of $f^{(i)}$ and $g^{(i)}$ yields the linear system

$$\begin{pmatrix}
x-1 & 1 & 0 & -2x-3 & -2 & 0\\
2x+1 & x+1 & 2 & -x-1 & -2x-4 & -4\\
x+1 & 2x+2 & x+3 & -x-2 & -x-2 & -2x-5\\
0 & x+1 & 2x+3 & 0 & -x-2 & -x-3\\
0 & 0 & x+1 & 0 & 0 & -x-2
\end{pmatrix}
\begin{pmatrix} u_0\\ u_1\\ u_2\\ v_0\\ v_1\\ v_2 \end{pmatrix} = 0.$$

This system has more variables than equations and must therefore have a nontrivial solution. Indeed, there is a solution vector $(u_0, u_1, u_2, v_0, v_1, v_2)$ with

$$\begin{aligned}
u_0 &= 2(x+1)(x^2+4x+5)(4x^2+9x+3),\\
u_1 &= 4x^5 + 21x^4 + 24x^3 - 42x^2 - 102x - 50,\\
u_2 &= (x+2)(4x^4 + 25x^3 + 56x^2 + 52x + 18),
\end{aligned}$$

and putting these values back into the ansatz gives a differential equation of order 4 with polynomial coefficients of degree 6 whose solution space contains both f and g and therefore also $f+g$:

$$(x+1)(x+2)(4x^4 + 25x^3 + 56x^2 + 52x + 18)h^{(4)}$$

$$\begin{aligned}
&+ (12x^6 + 103x^5 + 356x^4 + 628x^3 + 592x^2 + 286x + 58)h^{(3)} \\
&+ (20x^6 + 161x^5 + 521x^4 + 846x^3 + 702x^2 + 272x + 38)h'' \\
&+ (20x^6 + 157x^5 + 505x^4 + 826x^3 + 704x^2 + 296x + 52)h' \\
&+ (8x^6 + 54x^5 + 131x^4 + 88x^3 - 130x^2 - 216x - 80)h = 0.
\end{aligned}$$

2. Let us now compute a differential equation for the product $h = fg$. Make an ansatz

$$u_0 h + \cdots + u_4 h^{(4)} = 0$$

with unknown coefficients $u_0, \ldots, u_4$. The ansatz is equivalent to

$$\begin{aligned}
&u_0 fg + u_1(f'g + fg') + u_2(f''g + 2f'g' + fg'') \\
&\quad + u_3(f^{(3)}g + \cdots + fg^{(3)}) + u_4(f^{(4)}g + \cdots + fg^{(4)}) = 0,
\end{aligned}$$

and we can use the given differential equations to rewrite $f^{(4)}$, $f^{(3)}$, f'' and $g^{(4)}$, $g^{(3)}$, g'' in terms of f, f' and g, g'. This leads to

$$\begin{aligned}
&(u_0 - \tfrac{(3x^2+6x+1)}{(x+1)(x+2)}u_2 + \tfrac{(4x^2+4x-5)}{(x+1)(x+2)}u_3 + \tfrac{x(11x^3+45x^2+58x+23)}{(x+1)^2(x+2)^2}u_4)fg \\
&+ (u_1 - \tfrac{(4x^2+7x-3)}{(x+1)(x+2)}u_3 - \tfrac{(x+1)}{x+2}u_2 + \tfrac{(x-1)(17x+27)}{(x+1)(x+2)}u_4)fg' \\
&+ (u_1 - \tfrac{(3x^2+8x+7)}{(x+1)(x+2)}u_3 - \tfrac{(2x+1)}{x+1}u_2 + \tfrac{2(2x+1)(7x+9)}{(x+1)(x+2)}u_4)f'g \\
&+ (2u_2 - \tfrac{3(3x^2+7x+3)}{(x+1)(x+2)}u_3 + \tfrac{2(10x^2+15x+1)}{(x+1)(x+2)}u_4)f'g' = 0.
\end{aligned}$$

Equating the coefficients of fg, $f'g$, fg', $f'g'$ to zero gives the linear system

$$\begin{pmatrix}
1 & 0 & -\frac{3x^2+6x+1}{(x+1)(x+2)} & \frac{4x^2+4x-5}{(x+1)(x+2)} & \frac{x(11x^3+45x^2+58x+23)}{(x+1)^2(x+2)^2} \\
0 & 1 & -\frac{x+1}{x+2} & -\frac{4x^2+7x-3}{(x+1)(x+2)} & \frac{(x-1)(17x+27)}{(x+1)(x+2)} \\
0 & 1 & -\frac{2x+1}{x+1} & -\frac{3x^2+8x+7}{(x+1)(x+2)} & \frac{2(2x+1)(7x+9)}{(x+1)(x+2)} \\
0 & 0 & 2 & -\frac{3(3x^2+7x+3)}{(x+1)(x+2)} & \frac{2(10x^2+15x+1)}{(x+1)(x+2)}
\end{pmatrix}
\begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = 0.$$

This system has more variables than equations and therefore a nontrivial solution. A solution vector gives rise to the differential equation

$$\begin{aligned}
&(112x^8 + 1173x^7 + \cdots + 12588x + 2590)h \\
&+ (x+1)(x+2)(168x^6 + 1259x^5 + \cdots + 4183x + 1162)h' \\
&+ (x+1)^2(x+2)^2(119x^4 + 601x^3 + 1116x^2 + 1003x + 385)h''
\end{aligned}$$

$$+ 2(x+1)^2(x+2)^2(21x^4 + 118x^3 + 243x^2 + 233x + 91)h^{(3)}$$
$$+ (x+1)^2(x+2)^2(7x^4 + 44x^3 + 103x^2 + 112x + 49)h^{(4)} = 0,$$

whose solution space contains the product $h = fg$. □

In these examples, the bounds on the order are met. For the degrees, the bound is met for addition but not for multiplication. This reflects the typical behavior. As shown experimentally in Exercise 9, the order bounds are also generically tight, and the degree bound stated for addition is generically tight while the degree bound for multiplication appears to overshoot. Of course, for particular input, orders or degrees may be lower. An obvious example for addition is when we have $f = g$. In this case, $f + g = 2f$ satisfies the same differential equation as f (and g), and there is no need to double the order. For the multiplication, it happens less frequently that the order bound is not reached, but one case where this happens is again when $f = g$.

It is interesting to have a look at the singularities of the resulting differential equations. Observe that the differential equation computed for $f + g$ in the example above has singularities at -1 and -2. These singularities seem to be inherited from the given differential equations given for f and g, respectively. In addition, we find some new singularities at the roots of $4x^4 + 25x^3 + 56x^2 + 52x + 18$ which were not present in the input equations. These new singularities are apparent. To see this, let ξ be one of them. Since ξ is an ordinary point of both input equations, each of them has two linearly independent power series solutions, say f_1, f_2 and g_1, g_2, respectively. If we compute their first few terms, we can see that these four series are linearly independent over C, i.e., they generate a subspace of $C[[x]]$ of dimension 4. This subspace must be contained in the solution space of the differential equation computed in part 1 of Example 3.26, and in view of Theorem 3.20, it must then be equal to the solution space. According to Definition 3.17, this means that the singularities are apparent.

It is a common phenomenon that closure property operations introduce apparent singularities, but we can also use closure properties to eliminate apparent singularities.

Theorem 3.27 *Consider a differential equation $p_0 y + \cdots + p_r y^{(r)} = 0$ with polynomial coefficients $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$. Let $\xi \in C$ be a root of p_r, let E be some differential field extension of $C[[x-\xi]]$ with* $\mathrm{Const}(E) = C$ *such that the solution space V of the equation in E has dimension r.*

Then ξ is an apparent singularity of the differential equation if and only if there exists another linear differential equation with polynomial coefficients (possibly of higher order) for which ξ is an ordinary point and whose solution space in R contains V. □

Proof Let us denote the equation $p_0 y + \cdots + p_r y^{(r)} = 0$ by A and the other equation by B.

"$\Leftarrow$": Since ξ is an ordinary point of B, the dimension of its solution space in $C[[x-\xi]]$ matches the order of B (Theorem 3.16). By Theorem 3.20, the dimension of the solution space of B in E cannot be larger than the order of B, so all solutions of B in E are in fact in $C[[x-\xi]]$. In particular, all solutions of A in E are in $C[[x-\xi]]$, and since the solution space of A in E is assumed to have dimension r, Definition 3.17 implies that ξ is an apparent singularity of A.

"$\Rightarrow$": If ξ is an apparent singularity of A, then $V \subseteq C[[x-\xi]]$. Let $\{v_1, \ldots, v_r\}$ be a basis. We may assume that $v_i = (x-\xi)^{e_i} + \cdots$ for some pairwise distinct $e_i \in \mathbb{N}$, because if two basis elements have the same starting exponent, we can replace one of them by a linear combination in such a way that the dominant term cancels (similar to Gaussian elimination). Let $n = \max\{e_1, \ldots, e_r\}$ and let $U = \{1, 2, \ldots, n\} \setminus \{e_1, \ldots, e_r\}$. For every $u \in U$, the monomial $(x-\xi)^u$ satisfies the differential equation $(x-\xi)f'(x) - uf(x) = 0$. Therefore, by applying Theorem 3.25 $|U|$ times, we can construct a differential equation B of order $r + |U| = n$ whose solution space contains $V + \langle (x-\xi)^u : u \in U \rangle$. By the choice of U, this space has dimension n, and hence there cannot be any further solutions. Theorem 3.16 implies that ξ is an ordinary point of B. ■

Example 3.28 The solution space of the differential equation

$$2x(x+4)(x+1)^2 f''(x) - (x^2+8)(x+1)f'(x) + (x^2+2x+4)f(x) = 0$$

in $C[[x]]$ is generated by

$$1 + \tfrac{1}{2}x - \tfrac{1}{16}x^3 + \tfrac{11}{128}x^4 + \cdots \quad \text{and} \quad x^2 - x^3 + x^4 + \cdots .$$

Since the dimension of the solution space matches the order, the singularity 0 is apparent. Following the idea in the proof of Theorem 3.27, we can eliminate the singularity by computing a differential equation whose solution space is generated by the two power series above plus the additional solution $x \in C[[x]]$. Doing so gives

$$2(x^2-4x-8)(x+1)^2 f^{(3)}(x) + 3(x^2-8x-16)(x+1)f''(x) + 6xf'(x) - 6f(x) = 0.$$

We see that the singularity 0 has indeed disappeared.

But two new singularities have been introduced. We can get rid of them by noting that $\gcd(x(x+4), x^2-4x-8) = 1$ implies that there are polynomials $u, v \in C[x]$ with $x(x+4)u + (x^2-4x-8)v = 1$. We can find them with the extended Euclidean algorithm. A possible choice is $u = \frac{1}{24}(x-5)$, $v = \frac{1}{24}(x+3)$. Adding the product of u and the derivative of the given equation to the product of v and the equation we got from the closure property algorithm, we obtain

$$\begin{aligned} &2(x+1)^2 f^{(3)}(x) + \tfrac{1}{6}(x^3+2x^2-5x+36)(x+1)f''(x) \\ &\quad - \tfrac{1}{12}(x-1)(x^2-x+10)f'(x) + \tfrac{1}{12}(x^2-x+4)f(x) = 0. \end{aligned}$$

□

The closure properties of Theorem 3.25 apply not only to power series solutions of differential equations with polynomial coefficients. They hold more generally for equations with coefficients in a differential field K and solutions living in some differential ring R containing K. Of course, if the coefficients are not polynomials, the degree bounds have no meaning, but the bounds stated for the orders continue to hold.

Also the first closure property of the following theorem can be formulated more generally (Exercise 13). The other two concern operations which are not available in arbitrary differential rings.

Theorem 3.29 *Let $f \in C[[x]]$ be D-finite of order r and degree d.*

1. *f' is D-finite of order (at most) r and degree (at most) $2d$.*
2. *$\int f$ is D-finite of order (at most) $r+1$ and degree (at most) d.*
3. *If $g \in C[[x]]$ is algebraic, say $P(x, g) = 0$ for some nonzero polynomial $P \in C[x, y]$ with $\deg_y P \le r_g$, $\deg_x P \le d_g$, then the composition $f(g(x)) \in C[[x]]$ is D-finite of order (at most) rr_g.* □

Proof Let $p_0, \ldots, p_r \in C[x]$ with $p_r \neq 0$ and $\deg p_i \le d$ for all i be such that $p_0 f + \cdots + p_r f^{(r)} = 0$.

1. Differentiate the equation to obtain

$$p_0' f + (p_0 + p_1') f' + \cdots + (p_{r-1} + p_r') f^{(r)} + p_r' f^{(r+1)} = 0.$$

   The product of p_0' and the original equation minus the product of p_0 and this new equation gives an equation of order $r+1$ and degree $\le 2d$ which only contains $f', f'', \ldots, f^{(r+1)}$ but not f. Replacing $f^{(i)}$ by $g^{(i-1)}$ for a new unknown function g yields an equation of order r and degree $\le 2d$ with $g = f'$ among its solutions.
2. For $F = \int f$ we have $F' = f$, and therefore $p_0 F' + \cdots + p_r F^{(r+1)} = 0$.
3. Set $h = f \circ g$. By the chain rule, we have $h' = (f' \circ g) g'$, $h'' = (f'' \circ g)(g')^2 + (f' \circ g) g''$, etc. In general, the kth derivative of h is a linear combination of $(f \circ g), \ldots, (f^{(k)} \circ g)$ with coefficients in $C(x)[g, g', \ldots]$. Since f is D-finite of order r, we can even say that each $h^{(k)}$ ($k \in \mathbb{N}$) can be expressed as a certain linear combination of $(f \circ g), \ldots, (f^{(r-1)} \circ g)$ with coefficients in $C(x)[g, g', \ldots]$.
   According to Exercise 17 of Sect. 3.2, the derivation on $C(x)$ extends in a unique way to the field $C(x, g) \cong C(x)[Y]/\langle P \rangle$. Therefore, every element of $C(x)[g, g', \ldots]$ can be written as a $C(x)$-linear combination of $1, g, \ldots, g^{r_g - 1}$. Altogether, we find that all derivatives $h^{(k)}$ ($k \in \mathbb{N}$) belong to the $C(x)$-vector space generated by $(f^{(i)} \circ g) g^j$ for $i = 0, \ldots, r-1$ and $j = 0, \ldots, r_g - 1$. This implies that $h, h', \ldots, h^{(rr_g)}$ are linearly dependent over $C(x)$, as claimed. ■

For the third item, recall that the composition $f(g(x))$ is well-defined whenever $g(0) = 0$. This is however not a necessary condition. There is also the case when f is just a polynomial, and in this case the composition $f(g(x))$ is defined for all $g \in C[[x]]$. This includes in particular the case $f = x$, in which the claim reduces to the statement that every algebraic power series is D-finite. This case is sometimes refereed to as Abel's theorem.

Example 3.30 Let us compute a differential equation for $h(x) = \exp(x - x^2\sqrt{1-x}) \in \mathbb{Q}[[x]]$. The outer function $f(x) = \exp(x)$ satisfies the differential equation $f' - f = 0$ and the inner function $g(x) = x - x^2\sqrt{1-x}$ satisfies the polynomial equation $g^2 - 2xg + x^2(1 - x^2 + x^3) = 0$.

Differentiating the polynomial equation gives an equation in which g' appears linearly. Solving this equation for g' and rationalizing the denominator gives

$$g' = \frac{5x^4 - 4x^3 + 2x - 2g}{2(x-g)} = -\frac{3x-2}{2(x-1)} + \frac{5x-4}{2x(x-1)}g.$$

Taking also into account that $f' = f$, we have

$$\begin{aligned}
h &= h,\\
h' &= hg' = \Bigl(-\frac{3x-2}{2(x-1)} + \frac{5x-4}{2x(x-1)}g\Bigr)h,\\
h'' &= \Bigl(-\frac{3x-2}{2(x-1)} + \frac{5x-4}{2x(x-1)}g\Bigr)'h + \Bigl(-\frac{3x-2}{2(x-1)} + \frac{5x-4}{2x(x-1)}g\Bigr)h'\\
&= \Bigl(-\frac{25x^6 - 65x^5 + 56x^4 - 13x^2 - 12x + 8}{4(x-1)^2x} + \frac{20x^3 - 21x^2 - 8x + 8}{4(x-1)^2x^2}g\Bigr)h.
\end{aligned}$$

Making an ansatz $p_0h + p_1h' + p_2h'' = 0$ for unknowns $p_0, p_1, p_2 \in C[x]$, substituting the above expressions for h, h', h'' and equating coefficients of h and hg to zero leads to the linear system

$$\begin{pmatrix} 1 & -\frac{3x-2}{2(x-1)} & -\frac{25x^6-65x^5+56x^4-13x^2-12x+8}{4(x-1)^2x} \\ 0 & \frac{5x-4}{2(x-1)x} & \frac{20x^3-21x^2-8x+8}{4(x-1)^2x^2} \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ h_2 \end{pmatrix} = 0$$

with three variables and two equations. Its solution space is generated by a vector that gives rise to the differential equation

$$\begin{aligned}
&4(x-1)x(5x-4)h'' - 2(20x^3 - 21x^2 - 8x + 8)h'\\
&\quad + (125x^6 - 300x^5 + 240x^4 - 44x^3 - 6x^2 - 32x + 16)h = 0.
\end{aligned}$$

□

Conversely, if we are given a D-finite power series and want to know whether it is algebraic, the best approach in practice is to compute many series coefficients, guess a minimal polynomial using the techniques of Sect. 1.5, and then use closure properties to prove that the guess is correct. This works reasonably well if the power series under consideration is indeed algebraic. If it is not, proving its transcendence can be a hassle. There do exist algorithms which can find all of the algebraic solutions of a given differential equation, and the transcendence of a D-finite function can in principle be decided using such algorithms. However, these algorithms are so expensive that they have only been of theoretical interest so far.

In practice, it is often not difficult to collect strong evidence for a given D-finite power series to be transcendental. One piece of evidence is that guessing does not find a candidate for the minimal polynomial. This test is not very reliable, because even a small differential equation may have algebraic solutions with very large minimal polynomials. Another popular test checks the asymptotics of the series coefficients. It can be shown that an algebraic power series can only have coefficient sequences whose asymptotic behavior is described by a linear combination of terms of the form $\rho^n n^\alpha$ for some constant ρ and some $\alpha \in \mathbb{Q}$ which is not a negative integer. If the asymptotics do not have this form, the power series must be transcendental. To use this criterion, we can apply the techniques of Sect. 2.4 to the recurrence associated to the differential equation. If there are generalized series solutions that are incompatible with the asymptotic form of the coefficient sequences of algebraic power series, this is strong evidence, though not a formal proof, that the series at hand is transcendental.

A third useful test is based on generalized series solutions of differential equations, discussed in the following section. A differential equation which only has algebraic solutions cannot have any series solutions involving logarithmic or exponential terms, so the presence of series solutions involving logarithmic or exponential terms implies that the differential equation has at least some transcendental solutions. For an algebraic power series, it can be shown that the lowest order differential equation it satisfies has only algebraic solutions (cf. Exercise 16 in Sect. 4.4). So if we have a D-finite power series for which we know a certain differential equation and we know (or conjecture) that it does not satisfy any differential equation of lower order, and if the given differential equation has some generalized series solutions involving logarithmic or exponential terms, then we can conclude (or conjecture) that the given series is also transcendental. Of course, if all solutions at all singularities are free of logarithms and exponential terms, this does not mean that the series under consideration is algebraic. It only means that the test failed.

Here is another test, applicable for the case $C \subseteq \mathbb{C}$. Let's assume again that a D-finite power series is given by a differential equation of smallest possible order, so that the equation either has only algebraic solutions or none. Fix an ordinary point $\xi \in C$ of the differential equation and choose a closed path starting and ending at ξ and going around a singularity of the differential equation. Using the techniques of Sect. 3.1, we can numerically compute a matrix M such that whenever the vector v contains the values of the first few derivatives of a solution at the beginning of the path, Mv contains the corresponding values at the end of the path. If the solution is an algebraic function, all eigenvalues of M must be roots of unity, and while a numeric computation with finite precision can never prove that they are, it is usually easy to confirm numerically that they are not. Of course, if all eigenvalues of M are roots of unity, this does not mean that the series under consideration is algebraic. It only means that the test failed.

Let us return to closure properties. Closure properties are useful for proving identities. The basic idea for proving $A = B$ is to construct a differential equation for $A - B$ and then compare enough initial values to zero so that the whole series must be zero.

Example 3.31

1. The Airy functions $\mathrm{Ai}(x), \mathrm{Bi}(x)$ are defined as solutions of the differential equation $y'' - xy = 0$, with initial values $\mathrm{Ai}(0) = 3^{-2/3}\Gamma(2/3)^{-1}$, $\mathrm{Ai}'(0) = -3^{-1/3}\Gamma(1/3)^{-1}$, $\mathrm{Bi}(0) = 3^{-1/6}\Gamma(2/3)^{-1}$, $\mathrm{Bi}'(0) = 3^{1/6}\Gamma(1/3)^{-1}$. Let us prove the identity

$$\mathrm{Ai}(x)\mathrm{Bi}'(x) - \mathrm{Ai}'(x)\mathrm{Bi}(x) = 1/\pi.$$

First, from the defining differential equation for $\mathrm{Ai}(x)$ and $\mathrm{Bi}(x)$ we can compute differential equations that have their derivatives $\mathrm{Ai}'(x), \mathrm{Bi}'(x)$ as solutions. An application of Theorem 3.29 gives the equation $xy'' - y' - x^2y = 0$. Next, using Theorem 3.25, we can compute a differential equation whose solutions contain any product of one solution of $y'' - xy = 0$ with a solution of $xy'' - y' - x^2y = 0$. This gives the equation $y^{(4)} - 4xy'' - 10y' = 0$. By construction, $\mathrm{Ai}(x)\mathrm{Bi}'(x)$ and $\mathrm{Ai}'(x)\mathrm{Bi}(x)$ are solutions of this equation, therefore also their difference is. Using Theorem 3.5, we find that the coefficient sequence $(a_n)_{n=0}^{\infty}$ of any power series solution $y = \sum_{n=0}^{\infty} a_n x^n$ satisfies the recurrence $n(n+1)(n+2)(n+3)a_{n+3} - 2n(2n+3)a_n = 0$ $(n \in \mathbb{N})$. With this recurrence, it is clear that a solution is constant as soon as $a_1 = a_2 = a_3 = 0$. Since we can check

$$\mathrm{Ai}(x)\mathrm{Bi}'(x) - \mathrm{Ai}'(x)\mathrm{Bi}(x) = \frac{1}{\pi} + 0x + 0x^2 + 0x^3 + \mathrm{O}(x^4)$$

using the defining differential equation of $\mathrm{Ai}(x)$ and $\mathrm{Bi}(x)$ and the given initial values, the identity follows.

2. Let $a, b, c \in C$ be constants, c not a negative integer. The hypergeometric series ${}_2F_1\left(\begin{matrix} a, b \\ c \end{matrix} \,\middle|\, x\right)$ can be defined as the unique solution of the differential equation

$$x(1-x)y'' + (c - (a+b+1)x)y' - aby = 0$$

with initial value ${}_2F_1\left(\begin{matrix} a, b \\ c \end{matrix} \,\middle|\, 0\right) = 1$. The recurrence associated to this differential equation has order 1, so that a single initial value really suffices to determine the solution uniquely. We want to prove the identity

$$(1-x)^a {}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\,\middle|\,x\right) = {}_2F_1\left(\begin{matrix}a,c-b\\c\end{matrix}\,\middle|\,\frac{x}{x-1}\right).$$

The factor $(1-x)^a$ satisfies the differential equation $(1-x)y'+ay=0$. Applying Theorem 3.25 to this equation and the defining equation of ${}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\,\middle|\,x\right)$ gives

$$x(1-x)^2y'' - (x-1)(c+(a-b-1)x)y' - a(b-c)y = 0.$$

By construction, this equation has the left hand side $(1-x)^a {}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\,\middle|\,x\right)$ among its solutions. For the right hand side, consider $x/(x-1)$ as an algebraic function, defined by the polynomial equation $(x-1)y-x=0$, and apply Theorem 3.29 to this equation and the defining equation of ${}_2F_1\left(\begin{matrix}a,c-b\\c\end{matrix}\,\middle|\,x\right)$ (which is obtained from the defining equation of ${}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\,\middle|\,x\right)$ by replacing b with $c-b$). This gives again the equation

$$x(1-x)^2y'' - (x-1)(c+(a-b-1)x)y' - a(b-c)y = 0,$$

so by construction, this equation also has the right hand side ${}_2F_1\left(\begin{matrix}a,c-b\\c\end{matrix}\,\middle|\,\frac{x}{x-1}\right)$ among its solutions. Then also their difference is a solution. By inspection of the associated recurrence equation, it turns out that every power series solution is uniquely determined by its first term, so the proof of the identity is completed by noting that

$$(1-0)^a {}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\,\middle|\,0\right) = 1 = {}_2F_1\left(\begin{matrix}a,c-b\\c\end{matrix}\,\middle|\,\frac{0}{0-1}\right).$$

□

Algorithms for closure properties do not take into account the initial values of a power series but only the defining differential equation. As a consequence, the differential equations obtained via algorithms for executing closure properties are valid regardless of the choice of initial values. It is therefore possible that an equation constructed via closure properties for a certain D-finite power series may have a non-minimal order even if it was obtained from equations of minimal order.

Example 3.32 Consider the power series $f = \exp(x) + x$ and $g = 1 - \exp(x)$. We have the differential equations

$$(1-x)f'' + xf' - f = 0 \quad \text{and} \quad g'' - g' = 0.$$

Neither f nor g satisfies a first order equation. Using closure properties to construct from the two equations above an equation for $h = f + g$ gives

$$h''' - h'' = 0,$$

although h also satisfies the first order equation $(x + 1)h' - h = 0$. □

The example illustrates also that for a single D-finite function there are in general many differential equations it satisfies. If one equation is given, we can prove the correctness of other equations using closure properties. Suppose we know the equation

$$p_0 f + \cdots + p_r f^{(r)} = 0$$

and an appropriate number of initial values for f, and suppose we conjecture that also the equation

$$q_0 f + \cdots + q_s f^{(s)} = 0$$

holds, where s may be larger or smaller or equal to r. In order to prove the conjectured equation, define $g = q_0 f + \cdots + q_s f^{(s)}$ and use closure properties and the known equation to construct a differential equation for g. By checking an appropriate number of initial values of g, we can prove (or disprove) that $g = 0$. This proves (or disproves) the conjectured equation.

When we suspect that the execution of a closure property has given an equation of non-minimal order for a particular series at hand, we can search for a lower order equation by guessing and prove its correctness by the approach outlined above.

Exercises

1. Show that $\int \frac{\exp(x^2-3x)+\log(x-\sqrt{1-x^2})}{1-\sqrt{1+x^2}}dx$ is D-finite.

2. For $0 < z < 1$, the logarithmic integral $\mathrm{li}(z)$ is defined as $\mathrm{li}(z) = \int_0^z \frac{1}{\log(t)}dt$. Show that $\mathrm{li}(\exp(z))$ is D-finite.

3⋆. Prove the identity $F(a, b; 2b; x) = (1 - \frac{x}{2})^{-a} F(\frac{a}{2}, \frac{a+1}{2}; b + \frac{1}{2}; x^2/(2-x)^2)$.

4⋆⋆. For $\nu \in \mathbb{N}$, the ν-th Bessel function of the first kind is defined by $x^2 J_\nu''(x) + x J_\nu'(x) + (x^2 - \nu^2) J_\nu(x) = 0$ and the initial terms $J_\nu(x) = \frac{1}{2^\nu \nu!} x^\nu + 0x^{\nu+1} + \cdots \in \mathbb{C}[[x]]$. Prove the recurrence relation $x J_{\nu+2}(x) - 2(\nu + 1) J_{\nu+1}(x) + x J_\nu(x) = 0$ ($\nu \in \mathbb{N}$).

5⋆. Let $f, g \in C[[x]]$ be power series satisfying the differential equations $(x + 1) f'' + (2x + 3) f' + (x - 1) f = 0$, $(2x + 1) g'' + (3x + 2) g' + (x + 1) g = 0$. Compute differential equations for $f + g$ and fg.

6. The lowest order differential equation satisfied by x^2 is $xf' - 2f = 0$, and the lowest order differential equation satisfied by x^3 is $xf' - 3f = 0$. Using the algorithm behind Theorem 3.25, we find that $x^2 + x^3$ satisfies the differential equation $x^2 f'' - 4xf' + 6f = 0$. Why does it not find the first order equation $(x^2 + x)f' - (3x + 2)f = 0$?

7. Let $f \in C[[x]]$ be such that $(x+2)f'' + (3x+4)f' + (5x+6)f = 0$. Compute differential equations for $\int f$, f', and $f(x/(1-x))$.

8***.** Let $a_1, \dots, a_m \in C[[x]]$ be D-finite power series satisfying differential equations of respective orders $r_1, \dots, r_m$ and degrees $d_1, \dots, d_m$. Show that $a_1 + \cdots + a_m$ satisfies a differential equation of order $\sum_{i=1}^m r_i$ and degree $(1 + \sum_{i=1}^m r_i)(\sum_{i=1}^m d_i) - \sum_{i=1}^m r_i d_i$.

9. For various choices of r_a, r_b, d_a, d_b, define two D-finite power series $a, b \in C[[x]]$ via random initial values and random differential equations of orders r_a, r_b and degrees d_a, d_b, respectively. Using an efficient guessing program, find differential equations for $a+b$ and ab of smallest possible order. Apply multivariate polynomial interpolation (or linear algebra) to construct conjectures about how orders and degrees of these operators depend on r_a, r_b, d_a, d_b. Compare your results to the bounds stated in Theorem 3.25.

10. Prove or disprove: Every element of a Picard-Vessiot-extension of $C(x)$ is D-finite.

11***.** (Michael Singer) In Example 3.28, when we removed the singularity 0, why did the singularity -4 also disappear?

12***.** A differential equation A of order 2 has two power series solutions starting like $1 + 3x + 7x^2 - 2x^3 + 3x^4 + \cdots$ and $x + 2x^2 - \frac{9}{5}x^3 + 2x^4 + \cdots$, respectively. A differential equation B of order 2 has two power series solutions starting like $1 - x - x^2 + 3x^3 - x^4 + \cdots$ and $x + 2x^2 - 5x^3 - x^4 + \cdots$, respectively. Let C be the differential equation obtained by part 1 of Theorem 3.25. Show that while 0 is an ordinary point of both A and B, it is an apparent singularity of C.

13. Prove the following generalization of part 1 of Theorem 3.25: If K is a differential field, F is a D-module over K, and $f \in F$ is D-finite, then also $D(f)$ is D-finite.

14****.** Let K be an algebraic extension of $C(x)$ of degree d, and suppose that f satisfies a linear differential equation of order r with coefficients in K. Show that f also satisfies a linear differential equation of order (at most) dr with coefficients in $C(x)$.

15***.** Show that $f \in C[[x]]$ with $f(0) = 1$, $f'(0) = -3/8$ and $8(x-9)(x+1)^2 f''(x) - 2(x+31)(x+1)f'(x) + 3(x+11)f(x) = 0$ is algebraic.

16****.** Show that the equation $2xf(x) + \exp(x)(x+1)f(x)^2 + (2x-1)f'(x) = 0$ has a unique solution in $\mathbb{Q}[[x]]$ starting like $f(x) = 1 + x + 4x^2 + \frac{65}{6}x^3 + \cdots$, and prove that this series is D-finite.

17. Show that the composition of two D-finite functions is in general not D-finite.

18. Show that the multiplicative inverse of a D-finite function is in general not D-finite.

Hint: Consider $1/\log(x)$.

19. Show that the compositional inverse of a D-finite function is in general not D-finite.

20. The Hadamard product of two power series $f = \sum_{n=0}^{\infty} a_n x^n$, $g = \sum_{n=0}^{\infty} b_n x^n \in C[[x]]$ is defined as $f \odot g := \sum_{n=0}^{\infty} a_n b_n x^n$. Show that if f and g are D-finite, then so is $f \odot g$.

21. Show how the non-D-finiteness of $1/\log(x)$ implies the non-D-finiteness of $\log(\log(x))$ and $\sqrt{\log(x)}$.

22. Suppose that f is such that f'/f is algebraic. Show that f and $1/f$ are D-finite.

References

Abel's observation that every algebraic function is D-finite dates back to 1827, and other closure properties may also have been recognized around the same time. By 1894, the knowledge had already spread widely enough that Beke [52] didn't find it necessary to justify the claim that when $f_1, \ldots, f_n$ are D-finite functions and p is a polynomial in n variables, then $p(f_1, \ldots, f_n)$ is again D-finite. Closure properties also play a prominent role in the paper where Stanley coined the notion of D-finiteness [412]. The first systematic implementation of algorithms for closure properties was provided in the gfun package [379].

Closure properties are useful for showing that something is D-finite. To show that something is not D-finite can be much harder. One useful criterion of this sort is the following result by Harris and Sibuya [229]: for any function f, we have that both f and $1/f$ are D-finite if and only if f'/f is algebraic. Note that this statement also includes the converse of the statement proved in Exercise 22. Using this converse direction, it is easy to see with this criterion that $x/(\exp(x) - 1)$, the exponential generating function for the Bernoulli numbers, is not D-finite. Another criterion, also due to Harris and Sibuya [230], says that for two D-finite functions f, g such that $f = g^n$ for some n that is at least as large as the order of the defining differential equation for f, the function f'/f must be algebraic. For example, this implies that $\sqrt{1 + \exp(x)}$ is not D-finite. The first criterion admits the following analogous result for the recurrence case, which is due to Nishioka [336]: the two sequences f and $1/f$ are both D-finite if and only if f is an interlacing of D-finite sequences satisfying recurrence equations of order 1.

The process behind Theorem 3.27 is known as *desingularization*. The analogous process in the recurrence case is more subtle and was studied by Abramov, Barkatou, and van Hoeij [9, 11, 24]. More recent work on the subject is due to Chen, Jaroschek, Kauers, and Singer [136, 141, 249].

We have emphasized that applying closure properties algorithms to equations of minimal order for some D-finite functions f and g, the resulting equations for $f + g$ or fg are in general not of smallest possible order. However, the equations are minimal in some other sense, see the references given at the end of Sect. 4.1.

Computational aspects such as efficient algorithms for executing closure properties as well as bounds on the sizes of the resulting equations became interesting in the age of computer algebra. Bostan, Chyzak, Salvy, Lecerf and Schost considered these questions for differential equations for algebraic functions [83]. Kauers [265] worked out explicit bounds for the resulting orders and degrees for addition and multiplication, and Kauers and Pogudin give bounds for the equations satisfied by $f(g(x))$ where f is D-finite and g is algebraic [269]. Bronstein, Mulders, and Weil propose an efficient algorithm for the closure property "multiplication" [116]. Various techniques for implementing the closure property "addition" were compared by Bostan, Chyzak, Li, and Salvy [88].

A general algorithm for finding all algebraic solutions of a given linear differential equation with polynomial coefficients was given by Singer [406]. With the help of this algorithm, it can be decided whether a given D-finite power series is transcendental. Unfortunately, the complexity of Singer's algorithm is so high that it cannot be used in practice on any interesting example. That's why strong sufficient conditions for the transcendence of D-finite functions as described in the section are so important. A justification of the criterion based on asymptotics can be found in the book of Flajolet and Sedgewick [195]. Besides the tests mentioned in the text, there is another powerful test based on the so-called p-curvature of a differential equation. For any prime p, this is a certain matrix in $\mathbb{Z}_p^{r \times r}$ associated to a differential equation of order r, and it is the zero matrix for almost all p if the differential equation has only algebraic solutions. It is conjectured that the converse holds as well (Grothendieck-Katz conjecture), and if this is true, a nonzero p-curvature could be used to certify transcendence of a D-finite function if there is a way to recognize bad primes. Since almost all primes are not bad, the test can at least be used in practice to provide strong empirical evidence for the transcendence of a given D-finite function. Bostan, Caruso, and Schost present a fast algorithm for computing the p-curvature [93]. See the references given in their paper for further background.

3.4 Generalized Series Solutions

If 0 is an ordinary point of a differential equation of order r, then the solution space of the equation in $C[[x]]$ has the largest possible dimension r. We say that there is a complete set of solutions in this case. If 0 is a (non-apparent) singular point, then the dimension of the solution space in $C[[x]]$ is strictly less than r. We can think of this as a case of missing solutions. Where are they?

We already know from Sect. 3.2 that the missing solutions live in a certain differential field extension of $C[[x]]$. While this is a good answer in theory, it is not necessarily useful in practice, because it can be quite difficult to construct the required extension explicitly. In the present section, we take a different approach. The idea is to introduce a generalized kind of formal power series such that every differential equation has a complete set of solutions of this kind, and that we can calculate as many terms of these series as we want.

For computing a basis of the solution space in $C[[x]]$ (up to a given finite order), we have seen at the beginning of Sect. 3.2 that we can use the equivalence of bilateral series solutions and solutions in $C^{\mathbb{Z}}$ of the associated recurrence. We regarded formal power series as bilateral series $\sum_{n=-\infty}^{\infty} c_n x^n$ with $c_n = 0$ for all $n < 0$. Specifying $c_{-1} = c_{-2} = \cdots = 0$ as initial values, we used Algorithm 2.13 to construct a basis for the solution space in $C[[x]]$.

It is not much harder to find a basis of the solution space in the field $C((x))$ of formal Laurent series. These are bilateral series $\sum_{n=-\infty}^{\infty} c_n x^n$ such that there exists an $N \in \mathbb{Z}$ such that $c_n = 0$ for all $n < N$. Suppose the associated recurrence of the differential equation under consideration is

$$q_0(n)c_n + \cdots + q_j(n)c_{n+j} = 0.$$

We know from the discussion in Sect. 3.2 that if a solution of this recurrence is zero for all sufficiently small indices $n \in \mathbb{Z}$, the index N of its first nonzero term must be such that $N - j$ is a root of q_j. Since q_j is a polynomial, there are only finitely many roots, so there is an $N \in \mathbb{Z}$ such that $q_j(n - j) \neq 0$ for all $n < N$. Taking such an N and specifying initial values $a_{N-1} = a_{N-2} = \cdots = 0$, we can use Algorithm 2.13 as before in order to obtain a basis of the solution space in $C((x))$.

Example 3.33

1. The differential equation

$$25x^2 f''(x) - 10(2x - 5)xf'(x) - 3(7x^2 + 40x + 50)f(x) = 0$$

   has the associated recurrence

$$25n(n + 5)a_{n+2} - 20(n + 7)a_{n+1} - 21a_n = 0.$$

   The roots 0 and -5 of the leading coefficient polynomial imply that the only possible starting exponents of Laurent series solutions are 2 and -3. We can therefore find a basis of the solution space in $C((x))$ of the differential equation by finding all solutions $(a_n)_{n=-\infty}^{\infty}$ of the recurrence with $a_n = 0$ for all $n < -3$. Indeed, the solution space in $C((x))$ is generated by

$$x^{-3} - \tfrac{3}{5}x^{-2} + \tfrac{9}{50}x^{-1} - \tfrac{9}{250} + \tfrac{27}{5000}x + \tfrac{189}{250000}x^3 + \cdots$$
$$\text{and } x^2 + \tfrac{16}{15}x^3 + \tfrac{213}{350}x^4 + \tfrac{1261}{5250}x^5 + \cdots$$

2. The differential equation $2xf'(x) - f(x) = 0$ has the associated order-0 recurrence $(2n-1)a_n = 0$. Since $2n-1$ has no integer roots, it follows that the differential equation has no nonzero solutions in $C((x))$. □

The last example shows that by looking for solutions in $C((x))$, we still do not obtain a complete set of solutions in general. The example also gives a hint as to what is still missing. Its solution space is generated by $\sqrt{x}$. Note that $\sqrt{x} = x^{1/2}$ and $1/2$ is a root of the leading coefficient polynomial of the associated recurrence.

In general, whenever α is a root of the leading coefficient of the associated recurrence and the recurrence has order j, we can expect a series solution of the form $x^{\alpha-j}a(x)$, where a is a formal power series. Such series are called *Frobenius series*. They generalize formal Laurent series, but they are still not general enough to ensure that a differential equation of order r has r linearly independent solutions of this kind. There are two potential issues. One concerns the case where the leading coefficient polynomial has multiple roots or roots of integer distance. This situation can be handled by allowing logarithmic terms in the solution. The second issue is that the degree of the leading coefficient polynomial may be less than r. In this situation, we can get additional solutions by allowing exponential terms.

Altogether, we will show that when C is algebraically closed, then any linear differential equation of order r with polynomial coefficients admits r linearly independent solutions of the form

$$\underbrace{\boxed{\exp\bigl(s_1x^{-1/v}+s_2x^{-2/v}+\cdots+s_ux^{-u/v}\bigr)}}_{\text{exponential part}} \times \underbrace{\boxed{x^{\alpha}}}_{\text{polynomial part}} \underbrace{\boxed{\begin{aligned}&\Bigl(\bigl(c_{0,0}+c_{0,1}x^{1/v}+c_{0,2}x^{2/v}+\cdots\bigr)\\ &\underbrace{\boxed{\begin{aligned}&+\bigl(c_{1,0}+c_{1,1}x^{1/v}+c_{1,2}x^{2/v}+\cdots\bigr)\log(x)\\ &+\ \cdots\\ &+\bigl(c_{m,0}+c_{m,1}x^{1/v}+c_{m,2}x^{2/v}+\cdots\bigr)\log(x)^m\Bigr)\end{aligned}}}_{\text{logarithmic part}}\end{aligned}}}_{\text{series part}}$$

with $u, v \in \mathbb{N}$, $s_1, \ldots, s_u \in C$, $\alpha \in C$, $m \in \mathbb{N}$, and $c_{i,j} \in C$. We call these objects generalized series solutions.

In short, generalized series solutions have the form $\exp(p(x^{-1/v}))a(x^{1/v})$ for some $p \in C[x]$ with $p(0) = 0$ and some $a \in C[[[x]]]$. Recall from Definition 2.39 that the notation $C[[[x]]]$ refers to the ring of all finite C-linear combinations of series of the form $x^{\alpha}b(x, \log(x))$ with $\alpha \in C$ and $b \in C[[x]][y]$.

More generally, for a given point $\xi \in C$, we can ask for the generalized series solutions of the form $\exp(p((x-\xi)^{-1/v}))a((x-\xi)^{1/v})$ for some $p \in C[x]$ with $p(0) = 0$ and some $a \in C[[[x]]]$, or, in the case of $\xi = \infty$, for solutions of the form $\exp(p(x^{1/v}))a(x^{-1/v}, \log(x))$. As a change of variables can always bring us back to the case $\xi = 0$, it suffices to consider this case.

Computationally, generalized series solutions are constructed by first identifying the possible exponential parts and then computing for each such part the corresponding series solutions. The construction of the exponential parts is a recursive procedure where each recursion level produces a new coefficient s_i. At the base of the recursion, we obtain for each exponential part an auxiliary differential equation which has the corresponding series parts as solutions. Then we compute these series parts.

As the transformations applied during the recursion may introduce terms with fractional exponents into the coefficients of the differential equation, it is convenient to assume right away that the given differential equation has the form

$$p_0 f + \cdots + p_r f^{(r)} = 0$$

for some $p_0, \ldots, p_r \in C[x^{1/v}]$ with $p_r \neq 0$. Set $p_{i,j} = [x^{j/v}]p_i$ for $i = 0, \ldots, r$ so that $p_i = \sum_{j=0}^{d} p_{i,j} x^{j/v} = \sum_{j\in\mathbb{Z}} p_{i,j} x^{j/v}$ for $i = 0, \ldots, r$. We shall assume that $p_{i,0} \neq 0$ for at least one $i \in \{0, \ldots, r\}$. If this is not the case, we can obtain this property by multiplying the equation with an appropriate power of x.

Let us first discuss how to find solutions without exponential parts, i.e., solutions in $C[[[x]]]$. Consider a series $f(x) = \sum_{n=-\infty}^{\infty} c_n x^{n/v}$ with $c_n = 0$ for all sufficiently small $n \in \mathbb{Z}$. Plugging $f(x)$ into the differential equation gives a series of the same type, and equating its coefficients to zero gives a linear recurrence for c_n. A straightforward extension of the proof of Theorem 3.5 in order to cover the case $v \neq 1$ shows that we have

$$q_0(n)c_n + \cdots + q_{vr+d}(n)c_{n+vr+d} = 0$$

for all $n \in \mathbb{Z}$, where $q_j(x) = \sum_{i=0}^{r} p_{i,d+vi-j}\left(\frac{x+j}{v}\right)^{\underline{i}}$ for $j = 0, \ldots, vr + d$. The series f is a solution of the differential equation if and only if its coefficient sequence $(c_n)_{n=-\infty}^{\infty}$ is a solution of this recurrence. Sequence solutions which are zero for all sufficiently small indices $n \in \mathbb{Z}$ can start to become nonzero at indices which are determined by the leading coefficient polynomial of the recurrence. Usually this is q_{vr+d}, but not if this is the zero polynomial. In general, we must take q_j for the largest j such that q_j is not the zero polynomial. Observe that not all of the q_j can be zero.

Definition 3.34 Let $p_0, \ldots, p_r \in C[x^{1/v}]$, $p_r \neq 0$. Let $\xi \in C$. Write $p_i = \sum_{j=0}^{d} p_{i,j}(x - \xi)^{j/v}$ and define $q_j = \sum_{i=0}^{r} p_{i,d+vi-j}\left(\frac{x+j}{v}\right)^{\underline{i}} \in C[x]$ for $j = 0, \ldots, vr + d$. Let j be maximal such that q_j is not the zero polynomial. Then $\eta = q_j(x - j) \in C[x]$ is called the *indicial polynomial* at ξ of the differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$. If ξ is unspecified, it is understood that $\xi = 0$. □

Example 3.35 The differential equation $(x^2 - 3x)f''(x) + (6 - x^2)f'(x) + (3x - 6)f(x) = 0$ has the indicial polynomial $-3(x - 3)x$ at $\xi = 0$ if we take $v = 1$. □

The correspondence between series solutions of the differential equation and sequence solutions of its associated recurrence extends to sequence solutions with support in some offset $\alpha + \mathbb{Z} \subseteq C$ of the integers. If $(c_n)_{n\in\alpha+\mathbb{Z}}$ is a sequence $\alpha + \mathbb{Z} \to C$ such that $q_0(n)c_n + \cdots + q_{vr+d}(n)c_{n+vr+d} = 0$ for all $n \in \alpha + \mathbb{Z}$, then

$f(x) = \sum_{n\in\alpha+\mathbb{Z}} c_n x^{n/v}$ is a solution of the differential equation. The significance of the indicial polynomial η is that whenever $n \in \mathbb{Z}$ is minimal such that $c_{n+\alpha} \neq 0$ for a certain solution, then we have $\eta(n+\alpha) = 0$. Since η is a nonzero polynomial, it has at most finitely many roots, and so there are at most finitely many candidates for starting points.

In general, not every root of the indicial polynomial is a starting index of a Frobenius series solution. It can happen that a sequence solution that starts at a certain index cannot be continued across a later root of the indicial polynomial.

Example 3.36 Consider the differential equation $(x^3-3)xf''(x)+(6-5x^3)f'(x)+9x^2f(x) = 0$. Its associated recurrence is $(n-1)^2c_{n+2} - 3(n+2)(n+5)c_{n+5} = 0$, so the indicial polynomial is $\eta = -3(x-3)x$. The only possible starting terms of Frobenius series solutions are x^0 and x^3.

It is easily checked that the term x^3 itself is a solution of the differential equation. However, there is no series solution starting with x^0. To see why, try to compute one. Setting $f(x) = 1 + c_1x + c_2x^2 + \cdots$ and determining the coefficients through the recurrence first gives $c_1 = -\frac{25}{6}c_{-2} = 0$, $c_2 = -\frac{8}{3}c_{-1} = 0$, which is alright, but then for $n = -2$ the recurrence specializes to $9 - 0c_3 = 0$, which cannot be solved for c_3. □

Roots of the indicial polynomial indicate the starting indices and, as shown in the example above, also the possible terminating indices at which the computation of the coefficients of a series solution runs into a division by zero. Any truncated series solution with a truncation order later than the largest root of the indicial polynomial can be uniquely extended to an infinite series solution.

Like in Sect. 2.2, we can use deformed recurrence equations to avoid divisions by zero. Let q be transcendental over C and consider an ansatz for a series $f(x) = \sum_{n=-\infty}^{\infty} c_n x^{(n+q)/v}$ with $c_n = 0$ for all $n < 0$ and $c_0 = 1$. The terms $c_n \in C(q)$ for $n > 0$ are defined through the deformed recurrence

$$q_0(n+q)c_n + \cdots + q_{vr+d}(n+q)c_{n+vr+d} = 0.$$

For this series we have

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = \eta(q)x^{(q+d-j)/v},$$

where j is such that $\eta = q_j$ is the indicial polynomial (Exercise 4). The series f becomes a solution if we set q to a root of η, so that the right hand side vanishes. The only thing that might prevent us from doing so are poles in some of the rational functions $c_n \in C(q)$.

Writing the recurrence in the form $\eta(n+q)c_n = (\cdots)c_{n-1} + \cdots + (\cdots)c_{n-j}$, we see by induction that the denominator of c_n divides $\eta(q+1)\cdots\eta(q+n)$. If α is a root of $\eta(q)$, then there can be only finitely many $k \in \mathbb{N}$ such that α is also a root of $\eta(q+k)$. Therefore, for every root α of $\eta(q)$ there exists some $e \in \mathbb{N}$ such that $(q-\alpha)^e c_n \in C[q]$ for all $n \in \mathbb{N}$. For $g(x) = (q-\alpha)^e f(x)$ we have

$$p_0(x)g(x) + \cdots + p_r(x)g^{(r)}(x) = (q-\alpha)^e\eta(q)x^{(q+d-j)/v},$$

because $(q-\alpha)^e$ is free of x.

Now α is a multiple root of the right hand side, say of multiplicity $m \geq e$, so we can not only set $q = \alpha$ to obtain solutions, but also differentiate up to $m-1$ times with respect to q, using $\frac{d^i}{dq^i}x^{(q+d-j)/v} = \frac{1}{v^i}\log(x)^i x^{(q+d-j)/v}$, and then set q to α. In this way, we find generalized series solutions that may involve logarithmic terms. The procedure is summarized in the following algorithm.

Algorithm 3.37 *(See Algorithm 2.40 for the shift case)*
Input: $p_0, \ldots, p_r \in C[x^{1/v}]$, *with* $[x^0]p_i \neq 0$ *for at least one* $i \in \{0, \ldots, r\}$.
Output: $\deg\eta$ *many linearly independent solutions in* $\bigcup_{\alpha\in C} x^\alpha C[[x^{1/v}]][\log(x)]$ *of the differential equation* $p_0 f + \cdots + p_r f^{(r)} = 0$, *where* η *is the indicial polynomial of the differential equation. Each basis element is returned as a truncated series that admits a unique extension to a series solution.*

Set $j = 1 + vr + \max_{i=0}^r \deg p_i$ *and* $\eta = 0$.
while $\eta = 0$ *do*
    Set $j = j - 1$ *and* $\eta = \sum_{i=0}^r p_{i,d+vi-j}\left(\frac{x}{v}\right)^{\underline{i}} \in C[x]$.
Take $N \in \mathbb{N}$ *such that for any two roots* $\alpha, \beta \in C$ *of* η *with* $\alpha - \beta \in \mathbb{Z}$ *we have* $N > |\alpha - \beta|$.
Set $c_0 = 1$ *and recursively compute* $c_1, \ldots, c_N \in C(q)$ *such that for* $f(x) = \sum_{n=0}^N c_n x^{(n+q)/v}$ *we have* $p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = \eta(q)x^{(q+d-j)/v} + \mathrm{O}(x^{(q+d+N-j+1)/v})$.
Set $B = \emptyset$.
for all roots $\alpha \in C$ *of* η *do*
    Let k *be the multiplicity of* $x - \alpha$ *in* η.
    Find the smallest $e \in \mathbb{N}$ *such that* $q - \alpha$ *does not divide the denominator of* $(q-\alpha)^e c_n$ *for any* $n = 0, \ldots, N$.
    Set $B = B \cup \left\{\left[\frac{d^i}{dq^i}(q-\alpha)^e f(x)\right]_{q=\alpha} : i = e, \ldots, k+e-1\right\}$.
Return B.

Theorem 3.38 *(See Theorem 2.41 for the shift case) Algorithm 3.37 is correct. In particular:*

1. *If* C *is algebraically closed and* ℓ *is the degree of the indicial polynomial, the dimension of the solution space in* $C[[[x^{1/v}]]]$ *is at least* ℓ.
2. *If the indicial polynomial has a root of multiplicity* k, *then there is a solution involving logarithmic terms of degree at least* $k-1$.
3. *If the algorithm finds a solution involving logarithmic terms of degree* d, *then the indicial polynomial has certain roots* $\alpha_1, \ldots, \alpha_m \in C$ *with respective multiplicities* $k_1, \ldots, k_m \in \mathbb{N}$ *such that* $k_1 + \cdots + k_m > d$ *and* $\alpha_i - \alpha_j \in \mathbb{Z}$ *for all* i, j. $\square$

Proof First, because of the property of N ensured by line 4, every truncated series returned by the algorithm can be uniquely continued to a series solution. Therefore, every element of B indeed corresponds to a solution. Secondly, B is linearly independent, because every series in B starts with a different term $x^\alpha \log(x)^i$, and these terms are linearly independent. This completes the correctness proof.

1. This claim follows from the fact that line 10 supplies k new solutions for every root α of multiplicity k. If C is algebraically closed, then the sum of the multiplicities of the roots of η is equal to the degree of η.
2. This claim also follows from line 10, because we always have $e \geq 0$, and $[\frac{d^i}{dq^i}(q-\alpha)^e f(x)]_{q=\alpha}$ contains the nonzero term $i^{\underline{e}} v^{e-i} x^{\alpha/v} \log(x)^{i-e}$.
3. Because of line 10, a logarithmic term of degree m can only appear if $m < k + e$ for the values of k, e in some iteration of the main loop. Because of the recurrence for the coefficients c_n, the multiplicity of $q - \alpha$ in the denominator of some term c_n can exceed the multiplicity of $q - \alpha$ in the denominator of c_{n-1} by at most the multiplicity of $n - \alpha$ in η, for every $n \in \mathbb{N}$. Taking into account that $q - \alpha$ has multiplicity zero in the denominator of $c_0 = 1$, it follows that the number e determined in line 9 will be such that $k + e \leq k_1 + \ldots + k_m$. The claim follows. ■

Example 3.39

1. For the differential equation $(x^3 - 3)xf''(x) + (6 - 5x^3)f'(x) + 9x^2 f(x) = 0$ from the previous example we find

$$f(x) = x^q + 0x^{q+1} + 0x^{q+2} + \frac{(q-3)^2}{3q(q+3)}x^{q+3} + 0x^{q+4} + \cdots$$

   The factor q in the denominator of the coefficient of x^3 prevents us from setting $q = 0$. Since the indicial polynomial does not have any integer roots larger than 3, we know that none of the coefficients of the terms hidden in the $\cdots$ can have a denominator which contains q^2 as a factor. In the notation of Algorithm 3.37, this means we have $e = 1$.
   Setting $q = 0$ in $qf(x)$ gives a well-defined solution. It is the solution x^3 which we already know. The algorithm would find it in the iteration where it considers the root $\alpha = 3$, but not also in the iteration for $\alpha = 0$, because line 10 is limited to $i \geq e$.
   To get the missing solution, we differentiate $qf(x)$ with respect to q and then set $q = 0$. This gives $f(x) = 1 + 0x + 0x^2 + (\log(x) - 1)x^3 + 0x^4 + \cdots$. In fact, $1 + x^3 \log(x)$ happens to be an exact solution.
2. Consider the differential equation $4(x^2 + 1)x^2 f''(x) - 16x^3 f'(x) + (10x^2 + 1)f(x) = 0$. The associated recurrence is $2(2n^2 - 2n - 7)c_{n+2} + (2n+7)^2 c_{n+4} = 0$, so the indicial polynomial is $\eta = (2x - 1)^2$. Its double root $\alpha = 1/2$ predicts a solution involving logarithms ($k = 2$).
   Using the recurrence and the initial value $c_0 = 1$ we get the solution template

$$f(x) = x^q + 0x^{q+1} - \frac{2(2q^2 - 10q + 5)}{(2q+3)^2}x^{q+2}$$
$$+ 0x^{q+3} + \frac{4(2q^2 - 10q + 5)(2q^2 - 2q - 7)}{(2q+3)^2(2q+7)^2}x^{q+4} + \cdots$$

No denominators vanish when we set $q = 1/2$, so we can take $e = 0$ and obtain the solutions

$$\left[f(x)\right]_{q=1/2} = x^{1/2} - \tfrac{1}{16}x^{5/2} - \tfrac{15}{1024}x^{9/2} + \cdots$$
$$\left[\frac{d}{dq}f(x)\right]_{q=1/2} = \left(x^{1/2} - \tfrac{1}{16}x^{5/2} - \tfrac{15}{1024}x^{9/2} + \cdots\right)\log(x)$$
$$+ \left(\tfrac{17}{16}x^{5/2} + \tfrac{525}{2048}x^{9/2} + \cdots\right).$$

□

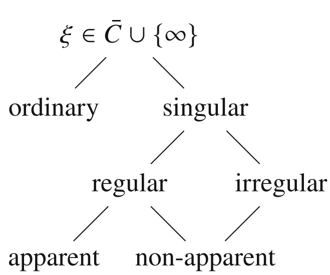
If the indicial polynomial has some roots whose difference is an integer, it is possible but not necessary that there are solutions involving logarithmic terms. For example, for an ordinary point the indicial polynomial is $x(x-1)\cdots(x-r+1)$, which has many roots at an integer distance but a perfectly nice set of power series solutions without logarithms.

If the degree of the indicial polynomial matches the order of the differential equation, Algorithm 3.37 provides us with a maximal set of linearly independent solutions. This situation arises sufficiently often to deserve its own terminology.

Definition 3.40 Let $p_0, \ldots, p_r \in C[x^{1/v}]$, $p_r \neq 0$.

1. A singularity $\xi \in C \cup \{\infty\}$ is called *regular* if the indicial polynomial for ξ has degree r. Otherwise it is called *irregular*.
2. The differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ is called *Fuchsian* if all of its singularities (in the algebraic closure of C and at infinity) are regular. □

Some authors use the word regular also in the sense of ordinary (i.e., no singularity), which can easily cause confusion. We avoid this use and restrict ourselves to the wording introduced in Definitions 3.14, 3.17, and 3.40 as summarized in the following diagram.



Example 3.41

1. The equation $xf'(x) - f(x) = 0$ is Fuchsian. Its only finite singularity is 0, and the solution $f(x) = x \in C[[[x]]]$ indicates that this singularity is regular. To see what happens at infinity, set $x = 1/z$ and $g(z) = f(1/z)$. Then $g'(z) = -\frac{1}{z^2} f'(1/z)$, and we get the equation $\frac{1}{z}(-z^2)g'(z) - g(z) = 0$, which has a singularity at $z = 0$. The solution $g(z) = 1/z \in C[[[z]]]$ indicates that this is a regular singularity, which implies that infinity is a regular singularity of the equation for $f(x)$.
2. The equation $x^2 f'(x) + f(x) = 0$ is not Fuchsian. Its singularity at 0 is irregular, because the indicial polynomial $\eta = 1$ has only degree 0, strictly less than the order of the equation.
3. The equation $f'(x) - f(x) = 0$ is not Fuchsian. It does not have any finite singularity, but there is a singularity at infinity, which turns out to be irregular. To see this, set $x = 1/z$ and $g(z) = f(1/z)$. Then $g'(z) = -\frac{1}{z^2} f'(1/z)$ and the equation transforms into $-z^2 g'(z) - g(z) = 0$, which, as we just saw, has an irregular singularity at $z = 0$. □

The indicial polynomial in general consists of contributions from various terms $x^i f^{(j)}(x)$ of the equation at hand. Each such term can contribute a polynomial of degree j. Therefore, whether the indicial polynomial has maximal degree or not depends on whether there is a contribution from a term $x^i f^{(r)}(x)$, where r is the order of the equation. The following theorem is a necessary and sufficient condition for this to be the case.

Theorem 3.42 *Let $\xi \in C$ and consider a linear differential equation*

$$p_0 f + \cdots + p_r f^{(r)} = 0$$

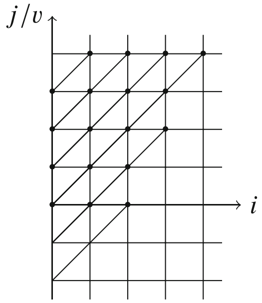
with coefficients $p_0, \ldots, p_r \in C[(x - \xi)^{1/v}]$, $p_r \neq 0$. Let μ_i be the multiplicity of $x - \xi$ in p_i, for $i = 0, \ldots, r$. Then ξ is a regular singularity if and only if $\mu_i - i \geq \mu_r - r$ for $i = 0, \ldots, r$. □

Proof Without loss of generality, we consider the case $\xi = 0$. Write $p_i = \sum_{j=\mu_i v}^{d} p_{i,j} x^{j/v}$ and let $j \in \{0, \ldots, vr + d\}$ be such that $\eta = \sum_{i=0}^{r} p_{i,d+vi-j} (x/v)^{\underline{i}}$ is the indicial polynomial of the equation. By the choice of j, we have $d + vi - j \leq v\mu_i$ for each i.

"$\Rightarrow$": If $\deg \eta = r$, then $p_{r,d+vr-j}$ must be nonzero, because the only term of degree r in the defining sum of η is the last summand. Therefore, $d + vr - j = v\mu_r$. Together with $d + vi - j \leq v\mu_i$ $(i = 0, \ldots, r)$ it follows that $\mu_i - i \geq \mu_r - r$ for $i = 0, \ldots, r$.

"$\Leftarrow$": If j is such that $p_{i,d+vi-j} \neq 0$ for some i, then $d + vi - j \geq v\mu_i$, so $d - j \geq v(\mu_i - i)$. By assumption, $\mu_i - i \geq \mu_r - r$ for all i, so $d - j \geq v(\mu_r - r)$ and then $d + vr - j \geq v\mu_r$. Since $p_{r,v\mu_r} \neq 0$ by definition of μ_r, it follows that $d + vr - j = v\mu_r$, which in turn implies that the coefficient of $(x/v)^{\underline{r}}$ in the defining sum of η is nonzero. Since all other summands represent polynomials of lower degree, it follows that $\deg \eta = r$. ■

The reasoning in the above proof becomes more transparent with the appropriate picture in mind. For each term $x^{j/v} f^{(i)}(x)$ in the differential equation, draw a point at position $(i, j/v)$ in the plane. If we set $f(x) = x^\alpha + \cdots$, we have $f^{(i)}(x) = \alpha^{\underline{i}} x^{\alpha-i} + \cdots$ and $x^{j/v} f^{(i)}(x) = \alpha^{\underline{i}} x^{\alpha-i+j/v} + \cdots$. If we draw a line of slope 1 from $(i, j/v)$ towards the left, it hits the vertical axis at height $-i + j/v$, which is exactly the exponent offset caused to the term x^α by the i-fold derivation and the multiplication by $x^{j/v}$.



The indicial polynomial is determined by the contributions which hit the vertical axis most deeply. Its degree is equal to the maximal contributing i, and we have a regular singularity (or an ordinary point) if and only if this happens to be $i = r$. This is not the case in the situation illustrated above, which corresponds to some equation of order $r = 4$ and an indicial polynomial of degree 2. When only a single term $x^{j/v} f^{(i)}(x)$ contributes to the indicial polynomial, as is the case in the situation depicted above, then the indicial polynomial is (a nonzero constant multiple of) $x^{\underline{i}}$. This generalizes the fact that the indicial polynomial is (a nonzero constant multiple of) $x^{\underline{r}}$ for 0 being an ordinary point. The indicial polynomial is different from a falling factorial $x^{\underline{i}}$ if and only if the lowest halfline in the picture passes through more than one point.

If the indicial polynomial does not have degree r, i.e., in the case of an irregular singularity, there are solutions involving nontrivial exponential parts. In order to see how to find them, first observe what differentiation does to a general term $x^\alpha e^{sx^c}$ with $c < 0$: we have

$$(x^\alpha e^{sx^c})' = (sc\, x^{\alpha+c-1} + \alpha\, x^{\alpha-1}) e^{sx^c}.$$

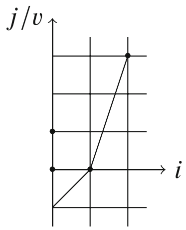
Inductively, this shows that plugging a single exponential term $x^\alpha e^{sx^c}$ into a term $x^{j/v} f^{(i)}(x)$ of the differential equation gives $(sc)^i x^{\alpha+i(c-1)+j/v} e^{sx^c} + \cdots$. Notice that the coefficient $(sc)^i$ does not depend on α because the assumption $c < 0$ implies that all terms with coefficients involving α get moved into the $\cdots$ part.

In order for $x^\alpha e^{sx^c}$ to be the first term of a generalized series solution f, we need the first terms $(sc)^i x^{\alpha+i(c-1)+j/v} e^{sx^c}$ of the generalized series $x^{j/v} f^{(i)}(x)$ to cancel each other when we plug them into the differential equation. Again, a diagram can help to clarify what is going on. Consider a fixed choice $c < 0$ and draw for each term $x^{j/v} f^{(i)}(x)$ a line of slope $1-c$ towards the left. The line will hit the vertical axis at height $-(1-c)i + j/v$, which is exactly the exponent offset caused to the term $x^\alpha e^{sx^c}$ by the i-fold derivation and the multiplication by $x^{j/v}$.

In the situation discussed previously, each term $p_{i,j} x^{j/v} f^{(i)}(x)$ on the lowest halfline in the picture contributed a term $p_{i,j}(x/v)^{\underline{i}}$ to the indicial polynomial. In the present situation, each such term contributes a term $p_{i,j}(sc)^i$ to the coefficient of the lowest degree term of the resulting series. The whole coefficient will thus be a nonzero polynomial in s, and its finitely many roots are the only values for s that can appear in the exponential term e^{sx^c} for the value c under consideration. Clearly, if this polynomial only consists of a single term, the only possible choice is $s = 0$, which corresponds to the empty exponential term $e^{0x^c} = 1$ and is therefore not of interest. To get a nontrivial polynomial for s, i.e., one with at least two terms, the lowest halfline in the picture must have contributions from at least two terms $x^{j/v} f^{(i)}(x)$, $x^{j'/v} f^{(i')}(x)$ of the differential equation. Since the halfline has slope $1-c$, we must then have $\frac{j'/v - j/v}{i'-i} = 1 - c$.

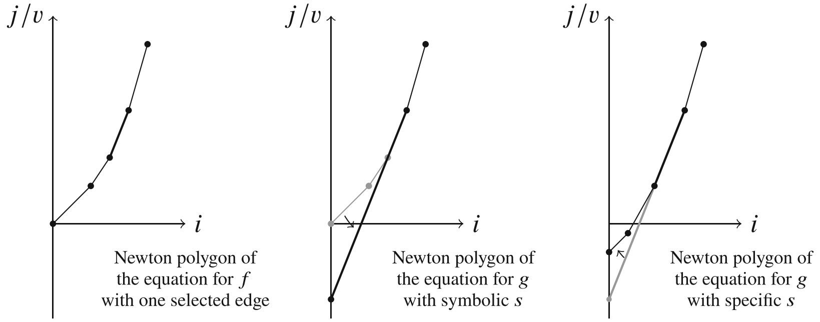
This observation allows us to determine the values for c that lead to a nontrivial equation for s, as follows. For every term $x^{j/v} f^{(i)}(x)$ of the differential equation at hand, draw a halfline in the plane that starts at $(i, j/v)$ and continues in the direction $(-1, -1)$, and determine the convex hull of all these halflines. The boundary of this convex hull is called the *Newton polygon* of the equation. The eligible values for c are precisely those for which the lower part of the Newton polygon has an edge of slope $1 - c$ with $c < 0$.

Example 3.43 Consider the differential equation $x^3 f''(x) + f'(x) + (x+1) f(x) = 0$. The Newton polygon of this equation is as follows.



The segment of slope 1 corresponds to the indicial polynomial x and the series solution $1 - x + \frac{1}{3}x^3 - \frac{1}{12}x^4 - \frac{9}{20}x^5 + \cdots$. The segment of slope 3 signals a solution with $c = -2$. To find the corresponding value(s) of s, plug $e^{sx^{-2}}$ into the equation. This gives $2s(2s-1)x^{-3}e^{sx^{-2}} + \cdots$, so the only nontrivial choice is $s = 1/2$. □

Every edge of the Newton polygon gives rise to a value of c, and for each such value, we get a polynomial equation for s that has one or more nonzero solutions. For a term e^{sx^c} determined in this way, we set $f(x) = e^{sx^c} g(x)$ for a new unknown function $g(x)$, plug this ansatz into the equation for f and divide it by e^{sx^c}. This leads to an equation for $g(x)$ with coefficients in $C[x^{1/v}]$ (possibly for a new v), which we want to solve recursively. In order to prove that the recursion terminates, we need to understand how the Newton polygon of the equation for g is related to the Newton polygon of the equation for f. The transition can be divided into two steps. In the first step, we keep s as a formal parameter. The coefficients in the equation for g then depend polynomially on this parameter s, and the Newton polygon for this equation is obtained from the Newton polygon of the equation for f by extending the edge of slope $1-c$ towards the left until it hits the vertical axis. In the second step, we set s to be one of the eligible values. This turns at least the coefficient of the lowest degree term on the vertical axis to zero, and possibly some others as well. Geometrically, it means that a part of the new segment breaks away and gets replaced by one or more less steep segments, as illustrated in the following figures.



The following lemma says that these picture accurately describe what happens. For convenience, we formulate it in terms of differential operators rather than for differential equations. A differential equation $p_0 f + p_1 f' + \cdots + p_r f^{(r)} = 0$ is written as an operator equation $L \cdot f = 0$ with an operator $L = p_0 + p_1 D + \cdots + p_r D^r$. The differential equation for g corresponds to the operator $\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$, where the two multiplications are understood to take place in the operator algebra. As remarked above and shown in Exercise 19, the coefficients of $\tilde{L}$ do not involve exponential terms.

Lemma 3.44 *(See Lemma 2.45 for the shift case) Let $c = \frac{u}{v} \in \mathbb{Q}$ be such that $c < 0$. Let L be a differential operator with coefficients in $C[x^{1/v}]$, and let $\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$. The coefficients of $\tilde{L}$ are understood as elements of $C[s][x^{1/v}, x^{-1/v}]$. Write*

$$L = \sum_{i=0}^{r} \sum_{j=0}^{d} p_{i,j} x^{j/v} D^i \quad \text{and} \quad \tilde{L} = \sum_{i=0}^{r} \sum_{j=v(c-1)r}^{d} \tilde{p}_{i,j} x^{j/v} D^i.$$

Let $j_0 \in \mathbb{Z}$ be minimal such that there exists some i with $j_0 - v(c-1)i \in \mathbb{N}$ and $p_{i,j_0 - v(c-1)i} \neq 0$. Let $i_{\min}$ be the smallest and $i_{\max}$ be the largest such i. Finally, let

$$\mu := \sum_{i=i_{\min}}^{i_{\max}} p_{i,j_0 - v(c-1)i} (cs)^i \in C[s].$$

Then we have

1. $\tilde{p}_{i,j} = 0$ *for all* (i, j) *with* $j < j_0 - v(c-1)i$.
2. $\tilde{p}_{i,j_0-v(c-1)i} = \frac{c^{-i}}{i!}\frac{d^i}{ds^i}\mu$ *for* $i = 0, \ldots, r$.
3. *If* μ *has a nonzero root of multiplicity* $i_{\max}$, *then* $vc \in \mathbb{Z}$. □

Proof According to the commutation rule for the derivation D, we have $Df = fD + f'$ for every f. More generally, by the binomial theorem, we have the commutation rule $D^i f = \sum_{k=0}^{i}\binom{i}{k} f^{(i-k)} D^k$. Using this commutation rule, we can calculate

$$\begin{aligned}
\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c} &= \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j} x^{j/v} \mathrm{e}^{-sx^c} D^i \mathrm{e}^{sx^c} \\
&= \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j} x^{j/v} \sum_{k=0}^{i}\binom{i}{k} \underbrace{\mathrm{e}^{-sx^c}(\mathrm{e}^{sx^c})^{(i-k)}}_{=(scx^{c-1})^{i-k}+\ldots} D^k \\
&= \sum_{k=0}^{r}\left(\sum_{i=k}^{r}\binom{i}{k}(cs)^{i-k} \underbrace{\sum_{j=0}^{d} p_{i,j}\left(x^{j/v-(1-c)(i-k)}+\cdots\right)}_{=p_{i,j_0+v(1-c)i}x^{j_0/v+(1-c)k}+\cdots}\right) D^k \\
&= \sum_{k=0}^{r}\left(\left(\underbrace{\sum_{i=k}^{r}\binom{i}{k} p_{i,j_0+v(1-c)i}(cs)^{i-k}}_{=\frac{c^{-k}}{k!}\frac{d^k}{ds^k}\mu}\right)x^{j_0/v+(1-c)k}+\cdots\right) D^k.
\end{aligned}$$

In the last step we used $\binom{i}{k} = \frac{i^{\underline{k}}}{k!}$. After exchanging i and k, claims 1 and 2 are proven.

For the third claim, suppose that $\mu = \tau(s-\sigma)^{i_{\max}}$ for some constants $\tau, \sigma \in C$. Then, by the binomial theorem, the coefficient of s^i in μ is nonzero for every $i = 0, \ldots, i_{\max}$. This means $p_{i,j_0-v(c-1)i} \neq 0$ for $i = 0, \ldots, i_{\max}$. Then $j_0 - v(c-1)i \in \mathbb{Z}$ for $i = 0, \ldots, i_{\max}$, and then $vc \in \mathbb{Z}$, as claimed. ■

In the notation of this lemma, we say that $i_{\max} - i_{\min}$ is the width of the edge of slope $1-c$ in the Newton polygon of L. Technically, the lemma doesn't require that the Newton polygon contains such an edge, but if it doesn't, we will have $i_{\max} = i_{\min}$, so we can think of this case as referring to an edge of width 0.

With the above lemma, we can now show that the recursive procedure alluded to before will terminate, and that it will produce a set of r linearly independent solutions for any given operator of order r.

Theorem 3.45 *(See Theorems 2.46 and 2.48 for the shift case) Suppose that C is algebraically closed. Consider a linear differential equation of order r with coefficients in $C[x^{1/v}]$. Then the differential equation has (at least) r linearly independent generalized series solutions of the form* $\exp(s_1 x^{c_1} + \cdots + s_m x^{c_m}) x^\alpha a(x)$ *with $s_1, \ldots, s_m \in C$, negative rational numbers $c_1, \ldots, c_m$, some constant $\alpha \in C$ and a series $a(x) \in C[[x^{1/w}]][\log(x)]$, for some $w \in \mathbb{N}$.* □

Proof By induction on i, we will show the following: for every differential equation whose Newton polygon contains an edge whose rightmost vertex lies on the vertical line through $(i, 0)$, there are at least i solutions of the announced type. The choice $i = r$ gives the theorem.

For the induction base $i = 0$, there is nothing to show. We will show that the claim is true for i provided that it is true for all smaller natural numbers. Consider an operator L for which the Newton polygon has an edge whose rightmost vertex lies on the vertical line through $(i, 0)$. If the slope of this edge is 1, then we get i linearly independent solutions from Theorem 3.38. If it is not 1, then it can only be greater than 1. In this case, let c be such that $1 - c$ is the slope of the edge under consideration, and consider the operator $\tilde{L} = \mathrm{e}^{-sx^c} L \mathrm{e}^{sx^c}$ and the polynomial $\mu \in C[s]$ of Lemma 3.44. Note that $\deg \mu = i$.

First consider the case when μ only has roots of multiplicity $< i$. Let $\sigma_1, \ldots, \sigma_m \in C$ be the nonzero roots of μ and let $e_1, \ldots, e_m$ be their multiplicities. Let $i_{\min}$ be the multiplicity of 0 in μ, so that $i_{\min} + e_1 + \cdots + e_m = i$. By the induction hypothesis, we obtain $i_{\min}$ many linearly independent solutions from the edges to the left of the current edge. Furthermore, setting s to be one of the roots σ_j in $\tilde{L}$ leads to an operator in which a part of length e_j of the extended edge is replaced by edges of flatter slope. Again by the induction hypothesis, we obtain e_j many linearly independent solutions of $\tilde{L}$ corresponding to these new edges. Multiplying them with $\mathrm{e}^{\sigma_j x^c}$ turns them into solutions of L. Altogether, we obtain $i = i_{\min} + e_1 + \cdots + e_m$ solutions. These solutions are linearly independent because the various linearly independent sets of series obtained through the induction hypothesis are multiplied by distinct dominant terms $\mathrm{e}^{\sigma x^c}$.

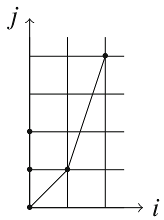
It remains to consider the case when μ has only a single root σ of multiplicity i. In this case, we have $vc \in \mathbb{Z}$ by part 3 of Lemma 3.44. Therefore, in this case the coefficients of $\tilde{L}$ again belong to $C[x^{1/v}]$ (after multiplying by a suitable power of x to clear any negative exponents if necessary). Setting s to be the unique root of μ will lead to a Newton polygon in which the entire edge of slope $1 - c$ is replaced by one or more flatter edges. Let $\tilde{c}$ be such that $1 - \tilde{c}$ is the slope of the rightmost new edge, let $\tilde{\tilde{L}} = \mathrm{e}^{-sx^{\tilde{c}}} \tilde{L} \mathrm{e}^{sx^{\tilde{c}}}$, and let $\tilde{\mu}$ be the corresponding polynomial as in Lemma 3.44. If $\tilde{\mu}$ has only roots of multiplicity $< i$, we can argue as before and obtain i linearly independent solutions of $\tilde{L}$. Multiplication by $\mathrm{e}^{\sigma x^c}$ turns them into solutions of L. If $\tilde{\mu}$ again has only a single root of multiplicity i, then $v\tilde{c} \in \mathbb{Z}$ by part 3 of Lemma 3.44, and thus the coefficients of $\tilde{\tilde{L}}$ still belong to $C[x^{1/v}]$ (after multiplying by a suitable power of x to clear any negative exponents if necessary). Because of $\tilde{c} \geq c + \frac{1}{v}$, after at most v repetitions of the argument, we either encounter an edge of width i and slope 1 (and then we can use Theorem 3.38) or we encounter a Newton polygon to which the argument of the previous paragraph applies. ■

Note that the proof shows more specifically that every edge of slope $1-c$ and width w gives rise to w linearly independent solutions with an exponential part whose dominant term is $e^{\sigma x^c}$ for some σ.

Note also that the set of all linear combinations of generalized series forms an integral domain. If we view it as a differential ring extension of $C[x^{1/v}]$, its constant field is C. Therefore, according to Theorem 3.20, a differential equation of order r with coefficients in $C[x^{1/v}]$ cannot have more than r linearly independent generalized series solutions, so every generalized series solution must be a C-linear combination of those identified by the theorem above. In particular, we can drop the "at least" from the statements of Theorems 3.38 and 3.45.

Example 3.46

1. Continuing Example 3.43, we have found one power series solution and the exponential term $\exp(\frac{1}{2}x^{-2})$ of a generalized solution of the equation $x^3 f''(x) + f'(x)+(x+1)f(x) = 0$. Setting $f(x) = \exp(\frac{1}{2}x^{-2})g(x)$, we obtain the equation $x^4 g''(x) - xg'(x) + (x^2+x+3)g(x) = 0$. This equation has the following Newton polygon:



The relevant edge for us is the edge of slope 1, which signals a solution without further exponential terms. It turns out to be $x^3(1+x+4x^2+\frac{17}{3}x^3+\frac{269}{12}x^4+\cdots)$, so the second solution of the original equation is $\exp(\frac{1}{2}x^{-2})x^3(1+x+4x^2+\cdots)$. The second edge need not be considered. In doing so, we would find the exponential term $\exp(-\frac{1}{2}x^{-2})$, and setting $g(x) = \exp(-\frac{1}{2}x^{-2})h(x)$ would just lead us back to the original equation, and we would only find the power series solution we already know. If we always consider all edges of the Newton polygon, we will descend into an infinite recursion.

2. Here is an example which leads to an exponential part consisting of more than one monomial. Consider the differential equation

$$x^8 f'''(x) + 4(2x^2+3)x^5 f''(x) + (29x^2+6x+36)x^2 f'(x) + 6(x^2-x+6)f(x) = 0.$$

Its Newton polygon is determined by the terms $f(x)$, $x^2 f'(x)$, $x^5 f''(x)$, and $x^8 f'''(x)$, so it has one edge of width 1 and slope 2 and one edge of width 2 and slope 3. We therefore expect one generalized series solution whose exponential

part starts with a term of the form $e^{sx^{-1}}$ and two linearly independent solutions with exponential parts starting with terms of the form $e^{sx^{-2}}$.
The solution starting with $e^{sx^{-1}}$ turns out to be $e^{x^{-1}}(1 - \frac{1}{36}x^2 - \frac{11}{108}x^3 + \cdots)$. Let us determine the remaining solutions. For the choice $c = -2$, the operator $\tilde{L}$ takes the form

$$\begin{aligned}\tilde{L} &= e^{-sx^{-2}} L e^{sx^{-2}} \\ &= x^8 D^3 + pD^2 + qD \\ &\quad + (-8s(s-3)^2 x^{-1} - 12(s-3) - 2(s-3)(2s-1)x + 6x^2 + 24sx^3)\end{aligned}$$

for certain polynomials $p, q \in \mathbb{Q}[x, s]$ which we suppress here. So the only choice for s is 3. Setting $s = 3$ gives the operator

$$L_1 = x^8 D^3 + 2x^5(4x^2 - 3)D^2 - x^3(13x - 6)D + 6x^2(1 + 12x),$$

whose generalized series solutions we determine recursively.
The Newton polygon for L_1 consists of the edges $(0,2)-(1,3)$, $(1,3)-(2,5)$, and $(2,5)-(3,8)$, whose slopes are 1, 2, and 3, respectively, and it indicates the possible choices $c = 0, -1, -2$. The choice -2 should be excluded because it would just bring us back to where we came from. The choice $c = 0$ leads to the series solution $x^{-1}(1 - \frac{73}{6}x + 73x^2 + \cdots)$ of the auxiliary operator. Multiplying this series with $e^{3x^{-2}}$ gives the second solution of the original equation.
For the choice $c = -1$ we consider the operator

$$\begin{aligned}\tilde{L}_1 &= e^{-sx^{-1}} L_1 e^{sx^{-1}} \\ &= x^6 D^3 + pD^2 + qD \\ &\quad + (-6s(s+1)x^{-1} - (s-2)(s^2 + 2s + 3) + 2(s^2 + 36)x + 10sx^2),\end{aligned}$$

where p, q are again two elements of $C[s, x]$ which we don't reproduce here. The only relevant value for s is -1, and for this choice, the operator simplifies to

$$L_2 = x^6 D^3 + x^3(8x^2 + 3x - 6)D^2 + 2x(5x^2 - 5x - 3)D - 2(-3 - 37x + 5x^2).$$

The Newton polygon of this operator has the edges $(0,0)-(1,1)$, $(1,1)-(2,3)$, and $(2,3)-(3,6)$, their slopes are 1, 2, and 3, respectively. We only need to consider the edge of slope 1, because the other two would only lead us back to the original equation. The edge of slope 1 signals a solution in $C[[[x]]]$ of L_2, and multiplication by $e^{-x^{-1}}$ turns it into a solution of L_1, which in turn becomes a solution of the original equation after multiplying by $e^{-3x^{-2}}$. Altogether, the third solution turns out to be

$$e^{3x^{-2} - x^{-1}} x^1 \big(1 + \tfrac{32}{3}x + \tfrac{112}{3}x^2 + \tfrac{704}{27}x^3 + \cdots\big).$$

□

Exercises

1. In Definition 3.34, show that a maximal j with $q_j \neq 0$ always exists, i.e., that the indicial polynomial is well-defined.

2. Show that j of Definition 3.34 is equal to $vr + d$ if and only if 0 is an ordinary point.

3.** Let L be a linear differential operator of order r with coefficients in $C[x^{1/v}]$. Show that $x^{r-q/v}(L \cdot x^{q/v})$ is an element of $C[q][x^{1/v}]$ and that the coefficient of the term with minimal exponent is the indicial polynomial for L.

4.** In the discussion preceding Algorithm 3.37, it is claimed that $p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = \eta(q)x^{(j+q)/v}$. Check this.

5. Show that $x^{1/3} + x^{1/5} + x^{1/7}$ satisfies a differential equation with polynomial coefficients of order 3, but none of lower order.

6. Why is $C[[[x^{-1}]]] = C[[x^{-1}]][\log x]$, not $= C[[x^{-1}]][\log(x^{-1})]$?

7. Show that the order of a differential equation with coefficients in $\mathbb{Q}[x]$ which has a solution of the form $x^{\sqrt{2}}\log(x)(1 + \cdots)$ must be at least 4.

8. Prove or disprove: If $\exp(x^{-7} + 28x^{-3} - 9x^{-1})(1 + \cdots)$ is a solution of a differential equation with polynomial coefficients, then the order of this equation must be at least 3.

9. Find the first few terms of the generalized series solutions of

a. $196x^3f''(x) - 14(28x^2 + 28x - 1)x^2f'(x) - (14x^2 - 30x + 441)f(x) = 0$

b. $100x^2f''(x) - 5(5x^2 + 10x + 64)xf'(x) + 2(17x^2 + 40x + 108)f(x) = 0$

c. $x^{12}f''(x) + (18x^4 + 10x^3 + 15x^2 - 32x + 20)x^6f'(x) + 2(10x^4 - 70x^3 + 203x^2 - 160x + 50)f(x) = 0$

10. Find the first few terms of the generalized series solutions at infinity of the three equations in the previous exercise.

11. Construct a differential equation of order 3 with coefficients in $\mathbb{Q}[x]$ which has a generalized series solution of the form $x^{5/2}(1 + \cdots) + x^{9/2}(3 + \cdots)\log(x) + x^{17/2}(11 + \cdots)\log(x)^2$.

12.** Consider a differential equation with coefficients in $C[x]$. Show that if f is a solution in $C[[x]][\log(x)]$ of degree m with respect to $\log(x)$, then also $[\log(x)^m]f \in C[[x]]$ is a solution of the differential equation.

13. Let $a_0, \ldots, a_m \in C[[x]]$, $p \in C[x]$, $\alpha \in C$ be such that

$$\exp(p(x^{-1}))x^{\alpha}(a_0(x) + a_1(x)\log(x) + \cdots + a_m(x)\log(x)^m)$$

is a generalized series solution of a certain differential equation with coefficients in $C[x]$. Show that $a_0, \ldots, a_m$ are D-finite.

14. Can a differential equation have a generalized series solution of the form $x^7(1+\cdots)+x^5\log(x)(1+\cdots)$, the point being that the starting exponent in the logarithmic part is smaller than the starting exponent of the logarithm-free part of the series?

15. Prove or disprove: If the indicial polynomial of a differential equation of order r is $cx^{\underline{r}}$ for some $c \in C \setminus \{0\}$, then 0 is an ordinary point.

16. Construct a linear differential equation with polynomial coefficients which has generalized series solution starting like

$$\mathrm{e}^{1/x}x^{1/2}\big(1+\tfrac{33}{8}x^2+\tfrac{403}{24}x^3+\tfrac{8211}{128}x^4+\tfrac{103251}{320}x^5+\tfrac{17277509}{9216}x^6+\cdots\big).$$

Hint: There is one of order two with polynomial coefficients of degree two.

17. What can be said about the exponential part and the logarithmic part of a generalized series solution of a differential equation of order 1 with polynomial coefficients?

18. A certain differential equation A has the Newton polygon $(0,0)-(1,1)-(2,3)$, another equation B has the Newton polygon $(0,0)-(1,1)-(2,4)$. Let C, D be the differential equations obtained by applying parts 1 and 2 of Theorem 3.25, respectively, to the equations A and B. What can be said about the Newton polygons of C and D?

19****.** Consider a differential equation $p_0 f+\cdots+p_r f^{(r)}=0$ with coefficients in $C[x^{1/v}]$. Show that substituting $f(x)=\exp(sx^{u/v})g(x)$ into this equation and dividing by $\exp(sx^{u/v})$ leads to a differential equation for $g(x)$ with coefficients in $C[s][x^{1/v}]$.

20. Show that x^x is not D-finite.

21*****.** Prove the commutation rule $D^n f=\sum_{k=0}^n\binom{n}{k}f^{(n-k)}D^k$.

22. Find the first few terms of a generalized series solution f of the inhomogeneous differential equation $f'(x)=\mathrm{e}^{sx^c}x^\alpha$.

23***.** Let p be a positive integer and consider a linear differential equation with coefficients in $C[x]$ (i.e., $v=1$). Suppose that the differential equation has a solution whose exponential part contains a term $\mathrm{e}^{\sigma x^{-u/p}}$ with $\gcd(u,p)=1$. Show that the order of the differential equation is at least p. Show also that if ω is a pth root of unity in C, then the differential equation also has a generalized series solution whose exponential part contains $\mathrm{e}^{\omega\sigma x^{-u/p}}$.

24***.** Suppose that C is algebraically closed. For a Fuchsian differential equation of order r with coefficients in $C[x]$ and a point $\xi \in C$, define the *defect* of the equation at ξ as $d(\xi)=\mathrm{Tr}(\eta)-\frac{1}{2}r(r-1)$, where η is the indicial polynomial at ξ and Tr denotes the trace of η, i.e., the sum of all roots of η, respecting multiplicities. For $\xi=\infty$, define $d(\xi)=\mathrm{Tr}(\eta)+\frac{1}{2}r(r-1)$. The *Fuchs relation* states that we have $\sum_{\xi\in C\cup\{\infty\}}d(\xi)=0$ for every Fuchsian differential equation. Note that $d(\xi)=0$

whenever ξ is an ordinary point, so the sum is actually finite. Confirm the Fuchs relation for the equation $6(x-3)(x-1)xf''(x)+(x^2-18x+9)f'(x)+(x+3)f(x)=0$.

25⋆. Find all $g \in C(x)$ such that $\log(g)$ is a solution of

$$19(x-4)(x-1)(x+1)(x+2)f'''(x)-2(6x^4-73x^3+339x+70)f''(x)$$
$$-6(2x^3-11x^2-32x+32)f'(x)=0.$$

Hint: What are the possible roots and poles of g?

26. Show that the differential equation

$$4(x-1)^2x^2f''(x)+4(x-1)(2x-1)xf'(x)-(7x^2-14x+8)f(x)=0$$

has no (nonzero) algebraic solutions.

References

The solution of linear differential equations in terms of generalized series goes back to the nineteenth century. Fuchs [198] recognized the different nature of regular and irregular singularities, his paper also contains the Fuchs relation discussed in Exercise 24. Frobenius [197] developed the method for finding solutions in $C[[[x]]]$, i.e., generalized series solutions without exponential part. The method for finding solutions involving exponential parts goes back to Fabry [185], who took inspiration from Puiseux' work on expanding algebraic functions into series [361, 362]. Puiseux had rediscovered an algorithm that Newton had already described in the seventeenth century [335]. In Newton's explanation, what we now call Newton polygon already appears as tabular arrangement of monomials.

For $C \subseteq \mathbb{C}$, analytic properties of generalized series are of interest. One motivation for Fuchs to introduce the distinction between regular and irregular singularities was that all the series solutions at a regular singularity converge in a neighborhood of the expansion point. A proof can be found in classical textbooks on differential equations, e.g., [247]. At an irregular singularity, in addition to solutions that cannot be expressed without exponential parts, we may have power series solutions which do not converge. For example, the solution space of the differential equation $x^2f''(x)-(3x+1)f'(x)+f(x)=0$ is generated by $\exp(-x^{-1})x^{-1}$ and the divergent power series $\sum_{n=0}^{\infty} n!x^n$. It is possible to give an analytic meaning to such solutions, but the techniques for doing so are beyond the scope of this book. The interested reader is referred to the books of Balser [39, 40] or to the book of Singer and van der Put [441].

3.5 Polynomial and Rational Solutions

For the remainder of this chapter, we consider algorithms for solving differential equations in closed form. In general, by a closed form we mean some expression which can be explicitly written down. There is no formal definition, and therefore also no general algorithm for finding closed forms. Instead, there are various classes of expressions, and for each of these, we can ask whether solutions from this class can be found algorithmically. For some kinds of expressions, this can be very difficult.

For the class of polynomials, it is not difficult. In order to find polynomial solutions of a prescribed maximal degree n, all we need to do is make an ansatz $f(x) = \sum_{k=0}^{n} a_k x^k$ with undetermined coefficients, plug the ansatz into the equation, equate like powers of x to zero, and solve the resulting linear system for the unknown coefficients $a_0, \dots, a_n$.

Example 3.47 Consider the differential equation

$$(333x^2+714x+335)f''(x)+2(125x^2-583x-754)f'(x)-10(125x-42)f(x) = 0.$$

We want to know all solutions in $C[x]$ of degree at most five. Consider an ansatz $f(x) = a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5$. Substituting $f(x)$ into the differential equation leads to

$$\begin{aligned}
&(1250a_5 - 250a_4)x^5 + (-500a_3 - 248a_4 + 6740a_5)x^4 \\
&\quad + (-750a_2 - 1080a_3 + 2536a_4 + 6700a_5)x^3 \\
&\quad + (-1000a_1 - 1246a_2 - 240a_3 + 4020a_4)x^2 \\
&\quad + (-1250a_0 - 746a_1 - 1588a_2 + 2010a_3)x \\
&\quad + (420a_0 - 1508a_1 + 670a_2) = 0.
\end{aligned}$$

Forcing the coefficients of x^k to zero leads to the linear system

$$\begin{pmatrix} 420 & -1508 & 670 & 0 & 0 & 0 \\ -1250 & -746 & -1588 & 2010 & 0 & 0 \\ 0 & -1000 & -1246 & -240 & 4020 & 0 \\ 0 & 0 & -750 & -1080 & 2536 & 6700 \\ 0 & 0 & 0 & -500 & -248 & 6740 \\ 0 & 0 & 0 & 0 & -250 & 1250 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = 0,$$

which has a solution space of dimension one generated by $(2, 5, 10, 11, 5, 1)$. It follows that all polynomial solutions of degree at most five are constant multiples of $x^5 + 5x^4 + 11x^3 + 10x^2 + 5x + 2$. □

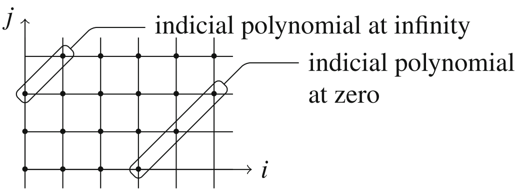
The equation $xf'(x) - nf(x) = 0$, which has the solution x^n, shows that the degree of a polynomial solution cannot only be bounded in terms of the order and the degree of the equation. However, for every given equation, there must be some finite $n \in \mathbb{N}$ such that all polynomial solutions of the equation have degree at most n. This is a consequence of Theorem 3.20, which says that the solution space of the equation in $C[x]$ is a C-vector space of finite dimension, so as soon as we have a basis of the solution space, we know that there is no polynomial solution whose degree exceeds the largest degree occurring among the basis elements.

A number $n \in \mathbb{N}$ such that every polynomial solution of a given equation has degree at most n is called a *degree bound* of the equation. In order to extract such a bound from an equation whose solution space in $C[x]$ is not yet known, note that every polynomial can also be viewed as an element of $C[[[x^{-1}]]]$, and that the techniques of the previous section allow us to compute the possible starting exponents of solutions in $C[[[x^{-1}]]]$. The degrees of polynomial solutions must be among them.

Instead of performing a change of variables to move the point at infinity to the origin so that the formulas of the previous section can be applied, let us work out explicitly what the indicial polynomial at infinity looks like.

Definition 3.48 Let $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$. Write $p_i = \sum_{j=0}^{d} p_{i,j} x^j$ and set $p_{i,j} = 0$ for $j < 0$ and $j > d$. Let $k \in \mathbb{Z}$ be maximal such that $\eta := \sum_{i=0}^{r} p_{i,k+i} x^{\underline{i}} \neq 0$. Then η is called the *indicial polynomial* at infinity of the differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$. □

Note that the indicial polynomial at infinity is determined by the high degree terms of the low order derivatives of an equation while the indicial polynomial at zero as defined in Definition 3.34 is determined by the low degree terms of the high order derivatives. A somewhat laborious calculation (Exercise 1) confirms that the indicial polynomials at zero and infinity are mapped to one another by the change of variables $x \mapsto 1/x$.



Proposition 3.49 *Let $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$, let $\eta \in C[x]$ be the indicial polynomial at infinity of the equation $p_0 f + \cdots + p_r f^{(r)} = 0$. Then for every polynomial solution $f \in C[x]$ of this equation we have $\eta(\deg f) = 0$.* □

Proof Write $p_i = \sum_{j=0}^{d} p_{i,j} x^j$ and set $p_{i,j} = 0$ for $j < 0$ and $j > d$, let $n = \deg f$ and write $f(x) = a_n x^n + \cdots$. Then $f^{(i)}(x) = a_n n^{\underline{i}} x^{n-i} + \cdots$, so $p_0(x) f(x) + \cdots + p_r(x) f^{(r)}(x) = \sum_{i=0}^{r} p_i(x)(a_n n^{\underline{i}} x^{n-i} + \cdots) = a_n (\sum_{i=0}^{r} p_{i,k+i} n^{\underline{i}}) x^{n+k} + \cdots = 0$, where k is as in Definition 3.48. The claim follows. ■

Example 3.50 The indicial polynomial at infinity of the equation considered in Example 3.47 is $\eta = 250(x - 5)$. Hence, the equation has no polynomial solutions other than those that we have already found. □

Not every nonnegative integer root of η must lead to a polynomial solution, but any nonnegative integer root may correspond to a polynomial solution. In this sense, the bound of Proposition 3.49 is sharp. This is a bit disappointing because η may have some very large roots. For example, the small equation $(x + 1)f'(x) - 1000f(x) = 0$ has the polynomial solution $(x + 1)^{1000}$, which is rather big in expanded form. Finding a basis for the space of polynomial solutions by linear algebra, as in Example 3.47, takes a number of operations in C which is cubic in the degree bound n (or $\mathrm{O}(n^{\omega})$ if we use fast linear algebra).

We can take advantage of the fact that polynomials are not only elements of $C[[x^{-1}]]$ but also elements of $C[[x]]$. Using the algorithms of Sect. 3.2, we can compute the first terms of a basis of the solution space in $C[[x]]$ and then determine the linear subspace which corresponds to the solution space in $C[x]$, as follows.

Algorithm 3.51 *(See Algorithm 2.51 for the shift case)*
Input: *$p_0, \ldots, p_r \in C[x]$ of degree at most d and with $p_r \neq 0$.*
Output: *A basis of the space of all $f \in C[x]$ with $\sum_{i=0}^{r} p_i f^{(i)} = 0$.*

1 *Choose $\epsilon \in C$ such that $p_r(\epsilon) \neq 0$.*
2 *Replace p_i by $p_i(x + \epsilon)$ for $i = 0, \ldots, r$.*
3 *Compute the indicial polynomial η at infinity (cf. Definition 3.48).*
4 *If η has no roots in $\mathbb{N}$, return $\emptyset$ and stop.*
5 *Let n be the largest integer root of η.*
6 *Compute the first $n + r + d$ terms of a basis of the solution space in $C[[x]]$ of the differential equation. Let $f_1, \ldots, f_r \in C[x]$ be the polynomials whose first $n + r + d$ terms agree with the respective terms of these basis elements. In other words, let f_i be the truncated series solutions, interpreted as polynomials.*
7 *Make an ansatz $f(x) = \alpha_1 f_1(x) + \cdots + \alpha_r f_r(x)$ with undetermined coefficients and equate the coefficients of x^k for $k = n + 1, \ldots, n + r + d$ to zero.*
8 *Solve the resulting linear system, and for each basis element $(\alpha_1, \ldots, \alpha_r)$ of its solution space, return $\alpha_1 f_1(x - \epsilon) + \cdots + \alpha_r f_r(x - \epsilon)$.*

Theorem 3.52 *Algorithm 3.51 is correct and apart from the cost of determining the integer roots of η, it needs no more than $\mathrm{O}(r^2(r+d)(n+r+d)+r\mathrm{M}(n))$ operations in C, where n is the largest integer root of η.* □

Proof In line 6, computing $n + r + d$ terms of r solutions of a recurrence of order $r + d$ and degree r can be done with $\mathrm{O}(r^2(r + d)(n + r + d))$ operations in C. In line 8, replacing x by $x - \epsilon$ in up to r polynomials of degree up to n costs no more than $\mathrm{O}(r\mathrm{M}(n))$ operations in C (cf. Theorem 1.21).

For the correctness, observe first that for all $f \in C[x]$ and all $\epsilon \in C$ we have $\sum_{i=0}^{r} p_i(x)f^{(i)}(x) = 0$ if and only if $\sum_{i=0}^{r} p_i(x+\epsilon)f^{(i)}(x+\epsilon) = 0$. This justifies the change of variables in lines 1 and 8. Now let V be the solution space in $C[x]$ of the differential equation and let W be the subspace of $C[x]$ generated by the output polynomials. We show that $V = W$.

"$\supseteq$": The associated recurrence has order at most $d + r$, and since 0 is an ordinary point after the change of variables applied in line 1, the leading coefficient polynomial of the associated recurrence does not have any roots in $\mathbb{N}$. Therefore, every solution $f \in C[[x]]$ in which at least $r + d$ consecutive coefficients are zero must be a polynomial.

"$\subseteq$": If f is a polynomial solution, then $\deg(f) \leq n$ by the choice of n, and f must be a certain linear combination of $f_1, \ldots, f_r$ because every polynomial solution is also a power series solution. This linear combination must appear in the solution space of the linear system computed in line 8. ■

The algorithm can be improved a bit, at least in practice, by unrolling the associated recurrence in the other direction. Instead of specifying initial values for the coefficients of $x^0, \ldots, x^{r-1}$ and then computing a full basis of the solution space in $C[[x]]$, we can specify as initial values that the coefficients of $x^{n+1}, \ldots, x^{n+r+d}$ should be zero, and then apply the recurrence backwards to compute a basis of the solution space in $C((x^{-1}))$ all the way down to the coefficient of $x^{-(r+d)}$. We can then find the linear combinations which contain no negative powers of x. If we are unlucky, this approach will also lead to the computation of r series solutions, so there is no gain in the worst case. However, since new solutions can only be born at integer roots of the trailing coefficients, and since a partial solution may also die at such points, it is fair to expect that we will typically have much fewer solutions, possibly just one.

Example 3.53 Consider the differential equation

$$\begin{aligned}&688(x-1)^2 f^{(5)}(x) + 63(x-1)^2 f^{(4)}(x) - (x-1)^3 f'''(x)\\&+ (2x-23)(23x-18) f''(x) - 556(x-4) f'(x) + 1920 f(x) = 0.\end{aligned}$$

The indicial polynomial at infinity is $(x - 5)(x - 12)(x - 32)$, so there may be polynomial solutions of degrees 5, 12, or 32. There are certainly five linearly independent power series solutions, and Algorithm 3.51 would compute the first 40 terms of each of these in line 6.

The associated recurrence of the differential equation can be written in the form

$$-(n-32)(n-12)(n-5)a_n = (\ldots)a_{n+1} + (\ldots)a_{n+2} + \cdots + (\ldots)a_{n+5}.$$

In order to compute a basis of the space of all solutions in $C^{\mathbb{Z}}$ which are zero for all sufficiently large indices, we start at $n = 32$ and have only one candidate solution whose terms can be computed by the recurrence all the way down to $n = 13$, but the attempt to compute the term for $n = 12$ leads to a division by zero, so the partial solution dies there. A new solution is born at $n = 12$ which can be continued all the way down to $n = 6$, but dies at $n = 5$. Finally, the solution born at $n = 5$ can be continued indefinitely. For this solution, it turns out that we have $a_{-1} =$

$a_{-2} = \ldots = a_{-8} = 0$, and therefore $a_n = 0$ for all $n < 0$. It is therefore the coefficient sequence of a polynomial solution of the differential equation, and all other polynomial solutions are constant multiples of it.

The solution is $x^5 - 30x^3 + 35x^2 + \frac{57705}{682}x - \frac{851181}{5456}$, and the total cost for finding it is equivalent to computing the terms of only one series solution in this example. □

Another observation about Algorithm 3.51 is that it recognizes the existence of polynomial solutions by solving a linear system that only involves a number of series terms that is independent of n. For very large n, it might be a good idea to first compute only the terms $a_{n+1}, \ldots, a_{n+d+r}$ of $f_1, \ldots, f_r$ using Algorithm 2.8, which only requires $\mathrm{O}(\sqrt{n})$ field operations. We can then solve the linear system, and if it happens to have no solution, there is no point in computing all of the remaining series terms.

In the case that the linear system does have solutions, we can conclude that the differential equation has polynomial solutions. In fact, the dimension of the solution space of the linear system matches the dimension of the solution space in $C[x]$ of the differential equation. However, at this point we do not know a basis of the solution space in $C[x]$. If we need one, there seems to be no way to avoid the computation of all terms of the series.

Fortunately, differential equations with indicial polynomials that have very large integer roots appear very rarely in applications. The more common situation is that the indicial polynomial does not have integer roots at all (and then there are no polynomial solutions), or that its integer roots have nearly the same size as r or d, so that the assumption that n is large compared to r or d is not adequate. Observe that the cost of Algorithm 3.51 is quartic in r while the cost of the naive algorithm is only cubic in r (assuming classical linear algebra). Most computer algebra systems today only use the naive algorithm.

We have remarked that there are no polynomial solutions if the indicial polynomial has no integer roots. It is easy to see that this is no longer the case when we turn to inhomogeneous equations. For example, consider the differential equation $f'(x) = x^2$. It obviously has the solution $f(x) = \frac{1}{3}x^3$, but its indicial polynomial is x and indicates only the constant solution. It remains true that we can find all solutions up to a specified degree d by making an ansatz, comparing coefficients, and solving a linear system over C. For an inhomogeneous equation, the linear system will be inhomogeneous, so the solution set may be empty or an affine space.

In order to turn the solution set of an inhomogeneous equation into a vector space, we can introduce a new parameter which is multiplied to the inhomogeneous part. Instead of solutions in $C[x]$ we are then looking for solutions in $C[x] \times C$, consisting of pairs (f, c) which are such that replacing the unknown function by f and the parameter by c makes the equation true. Besides getting back into the realm of vector spaces, homogenization allows us to handle several inhomogeneous parts at the same time. We simply take as the right hand side a formal linear combination of the inhomogeneous parts with parameters as coefficients. In summary, we consider the following problem: given $p_0, \ldots, p_r \in C[x]$ and $g_1, \ldots, g_m \in C[x]$, we want to find all tuples $(f, c_1, \ldots, c_m) \in C[x] \times C^m$ such that

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = c_1 g_1(x) + \cdots + c_m g_m(x).$$

Such an equation is called a *parameterized linear differential equation.*

Example 3.54

1. The solution space in $C[x] \times C^2$ of the parameterized differential equation

$$(x + 1)f(x) + (x + 2)f'(x) + (x + 3)f''(x) = c_1(x + 4)^2 + c_2(x + 6)^2$$

is generated by $(2x + 8, 3, -1)$.

2. The solution space in $C[x] \times C^2$ of the parameterized differential equation

$$(x + 1)f(x) - \tfrac{3}{2}(x + 2)^2 f'(x) + (x + 3)^3 f''(x) = c_1(x + 4) + c_2(x + 6)$$

is generated by $(x^2 + 14x, -69, 41)$ and $(2, 5, -3)$. □

Degree bounding for the parameterized case relies on the following generalization of Proposition 3.49.

Proposition 3.55 *Let $p_0, \ldots, p_r \in C[x]$, $p_r \neq 0$ and let $d = \max_{i=0}^{r}(\deg_x(p_i) - i)$. Let η be the indicial polynomial at infinity of the differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$. Let $f \in C[x]$ and $n = \deg_x(f)$. If*

$$\deg_x(p_0 f + \cdots + p_r f^{(r)}) < n + d,$$

then $\eta(n) = 0$. □

Proof Write $p_i = \sum_{j=0}^{d+i} p_{i,j} x^j$ and set $p_{i,j} = 0$ for $j < 0$ and $j > d + i$. By the choice of d we have $\eta = \sum_{i=0}^{r} p_{i,d+i} x^{\underline{i}}$. Writing $f(x) = a_n x^n + \cdots$ and using $f^{(i)}(x) = a_n n^{\underline{i}} x^{n-i} + \cdots$, we get

$$\begin{aligned} p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) &= \sum_{i=0}^{r} p_i(a_n n^{\underline{i}} x^{n-i} + \cdots) \\ &= a_n \sum_{i=0}^{r} p_{i,d+i} n^{\underline{i}} x^{n+d} + \cdots , \end{aligned}$$

and by the assumption on the degree, it follows that $\eta(n) = 0$. ■

Algorithm 3.56 *(See Algorithm 2.56 for the shift case)*
Input: $p_0, \ldots, p_r \in C[x]$ *and* $g_1, \ldots, g_m \in C[x]$.
Output: *A basis of the C-vector space of all $(f, c_1, \ldots, c_m) \in C[x] \times C^m$ such that*

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = c_1 g_1(x) + \cdots + c_m g_m(x).$$

1 *Compute the indicial polynomial* η *at infinity of the differential equation* $p_0 f + \dots + p_r f^{(r)} = 0$, *and let* $\xi_1, \dots, \xi_k$ *be its roots in* $\mathbb{N}$ *(if there are any).*

2 *Set* $d = \max_{i=0}^{r}(\deg_x(p_i) - i)$ *and* $n = \max\{\xi_1, \dots, \xi_k, \max_{i=1}^{n} \deg_x(g_i) - d\}$.

3 *Make an ansatz* $f(x) = f_0 + f_1 x + \dots + f_n x^n$ *with undetermined coefficients* $f_0, \dots, f_n$ *and compute*

$$p_0 f + \dots + p_r f^{(r)} - c_1 g_1 - \dots - c_m g_m$$

with undetermined coefficients $c_1, \dots, c_m$.

4 *Equate the coefficients of* x^i $(i = 0, \dots, n + d)$ *in this polynomial to zero and solve the resulting linear system for* $f_0, \dots, f_n, c_1, \dots, c_m$. *For each solution, return* $(f_0 + \dots + f_n x^n, c_1, \dots, c_m) \in C[x] \times C^m$.

Theorem 3.57 *Algorithm 3.56 is correct.* □

Proof It is clear that every output tuple is indeed a solution, that these solutions are linearly independent, and that at least all solutions with $\deg_x(f) \le n$ must be C-linear combinations of the returned solutions. It therefore suffices to show that there cannot be any solutions with $\deg_x(f) > n$. Indeed, for any choice of $c_1, \dots, c_m$, the right hand side of the differential equation is a linear combination of $g_1, \dots, g_m$ and hence a polynomial of degree at most $\max_{i=1}^{m} \deg_x(g_i)$. If $(f, c_1, \dots, c_m) \in C[x] \times C^m$ is a solution, then we must have $\deg_x \sum_{i=0}^{r} p_i f^{(i)} \le \max_{i=1}^{m} \deg_x(g_i)$. By Proposition 3.55, if we have $\deg_x(f) - d > \sum_{i=1}^{n} \deg_x(g_i)$, then $\deg_x(f)$ is a root of η. The claim follows. ■

The solution algorithm for parameterized equations is not restricted to the linear algebra approach and can also be combined with the idea of Algorithm 3.51, which may be a good alternative in situations where n is large compared to r and d. In addition to the series solutions of the homogeneous equation computed in Algorithm 3.51, we also have to compute for each g_i one particular series solution of the inhomogeneous equations with g_i as right hand side. Since 0 is an ordinary point of the left hand side (after performing a suitable change of variables if necessary), a series solution exists for every right hand side (see Exercise 2 of Sect. 3.2). The inhomogeneous differential equation translates into an inhomogeneous associated recurrence by which the terms of the particular series solution can be computed as discussed in Sect. 2.1 (cf. Exercises 2 and 3 of this section). We finally obtain the series terms of r linearly independent series solutions of the homogeneous differential equations as well as m particular solutions of the m inhomogeneous differential equations with the respective right hand sides $g_1, \dots, g_m$. We can then continue as in Algorithm 3.51 and compute the C-linear combinations that cancel all coefficients beyond the degree bound. These correspond to the solutions of the original parameterized equation.

Example 3.58 Consider again the parameterized equation

$$(x+1)f(x) - \tfrac{3}{2}(x+2)^2 f'(x) + (x+3)^3 f''(x) = c_1(x+4) + c_2(x+6).$$

In the notation of Algorithm 3.56 we have, $d = 1$ and $n = 2$. The associated recurrence of the homogeneous equation has order 3. We compute series solutions with truncation order 5. As solutions of the homogeneous equation, we may find the basis elements

$$f_1 = 1 - \tfrac{1}{54}x^2 - \tfrac{1}{729}x^3 + \tfrac{53}{52488}x^4 - \tfrac{1103}{2361960}x^5 + \cdots,$$
$$f_2 = x + \tfrac{1}{9}x^2 + \tfrac{1}{486}x^3 - \tfrac{31}{17496}x^4 + \tfrac{83}{98415}x^5 + \cdots,$$

and solving the two inhomogeneous cases with respective right hand sides $x+4$ and $x+6$, we may find

$$f_3 = \tfrac{2}{27}x^2 - \tfrac{19}{1458}x^3 + \tfrac{55}{13122}x^4 - \tfrac{3391}{2361960}x^5 + \cdots,$$
$$f_4 = \tfrac{1}{9}x^2 - \tfrac{11}{486}x^3 + \tfrac{67}{8748}x^4 - \tfrac{2129}{787320}x^5 + \cdots.$$

We now set up a linear system for finding the linear combinations of $f_1, \ldots, f_4$ that make the coefficients of x^3, x^4, x^5 vanish: the solution space of

$$\begin{pmatrix} -\frac{1}{729} & \frac{1}{486} & -\frac{19}{1458} & -\frac{11}{486} \\ \frac{53}{52488} & -\frac{31}{17496} & \frac{55}{13122} & \frac{67}{8748} \\ -\frac{1103}{2361960} & \frac{83}{98415} & -\frac{3391}{2361960} & -\frac{2129}{787320} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ c_1 \\ c_2 \end{pmatrix} = 0$$

has the basis $\{(2, 0, 5, -3), (13, 7, -2, 1)\}$. It follows that

$$\{(2f_1 + 5f_3 - 3f_4, 5, -3), (13f_1 + 7f_2 - 2f_3 + f_4, -2, 1)\} \subseteq C[x] \times C^2$$

is a basis of the solution space of the parameterized differential equation. □

We continue with discussing how to find solutions in $C(x)$ rather than in $C[x]$. We reduce the problem of finding rational solutions to the problem of finding polynomial solutions of an auxiliary equation, which we can solve by one of the algorithms described so far. Consider a parameterized differential equation

$$p_0 f + \cdots + p_r f^{(r)} = c_1 g_1 + \cdots + c_m g_m$$

with known $p_0, \ldots, p_r, g_1, \ldots, g_m \in C[x]$ and unknown $c_1, \ldots, c_m \in C$ and $f \in C(x)$. We may assume that $p_r \neq 0$. It is fair to assume that the p_i and the g_i are polynomials rather than rational functions, because we are free to multiply a given equation with a common denominator if needed. Allowing the unknown function f to have a denominator is a more substantial generalization, unless somebody explicitly tells us the denominator of f. If we know a polynomial $v \in C[x]$ such that there is a solution $(f, c_1, \ldots, c_m) \in C(x) \times C^m$ with $vf \in C[x]$, i.e., where v is (a multiple of) the denominator of f, then we can substitute $f = u/v$ for an unknown polynomial u into the equation, clear denominators, and obtain a parameterized differential equation for u. Every solution $(u, c_1, \ldots, c_m) \in C[x] \times C^m$ of this auxiliary equation translates into a solution $(u/v, c_1, \ldots, c_m) \in C(x) \times C^m$ of the original equation. The question is thus how to find the possible denominators of rational solutions. In view of Theorem 3.20 it is clear that for every given equation there exists a finite common denominator of all its solutions. This motivates the following definition.

Definition 3.59 Let $p_0, \ldots, p_r, g \in C[x]$, $p_r \neq 0$, and let $v \in C(x)$ be such that for every $f \in C(x)$ with

$$p_0 f + \cdots + p_r f^{(r)} = g$$

we have $vf \in C[x]$. Then v is called a *universal denominator* or a *denominator bound* for the equation. □

Assume for the moment that C is algebraically closed. In order to construct a universal denominator $v = (x - \xi_1)^{e_1} \cdots (x - \xi_k)^{e_k} \in C[x]$, we need to identify its roots $\xi_1, \ldots, \xi_k$, and for each root ξ_i an upper bound on its multiplicity e_i. It turns out that both parts of the job are rather straightforward. For the roots of v, we claim that they must be singularities of the equation, i.e., roots of p_r. To show this, note that whenever $f \in C(x)$ has a pole of multiplicity e at ξ, then $f^{(i)}$ has a pole of multiplicity $e + i$, for every $i \in \mathbb{N}$. This can be seen for example by considering the partial fraction decomposition of f. In order for f to be a solution of a parameterized differential equation, the left hand side $p_0 f + p_1 f' + \cdots + p_r f^{(r)}$ must be equal to the right hand side, which is just a polynomial. Since the p_i are polynomials too, the multiplicity of the pole ξ in $p_0 f + \cdots + p_{r-1} f^{(r-1)}$ can be at most $e + r - 1$, and hence the multiplicity of the pole ξ in $p_r f^{(r)}$ can also be at most $e + r - 1$, for otherwise there is no chance for the poles on the left hand side to cancel out. But since $f^{(r)}$ has a pole of multiplicity $e + r$ at ξ, it follows that p_r must have at least a single root at ξ, which is what we wanted to show.

For homogeneous equations there is also a more direct, but less explicit, argument: if f is a rational solution of such an equation, then its Laurent series expansion in $C((x - \xi))$ must be a solution too, for any choice $\xi \in C$. If ξ is a pole of f, then at least one of the solutions in $C((x - \xi))$ does not belong to $C[[x - \xi]]$, so ξ cannot be an ordinary point of the differential equation, and so it must appear among the roots of p_r.

For homogeneous equations, the same reasoning also provides us with bounds on the multiplicities. Clearly, if f is a rational solution with a pole of multiplicity e at $\xi \in C$, then the expansion of f in $C((x - \xi))$ is a formal Laurent series solution with starting exponent $-e$, and so $-e$ must be a root of the indicial polynomial at ξ of the homogeneous equation. Letting thus $\xi_1, \ldots, \xi_k$ be the roots of p_r and setting e_i to the largest integer such that $-e_i$ is a root of the indicial polynomial at ξ_i (taking $e_i = 0$ if the indicial polynomial has no integer roots), we have that $v = (x - \xi_1)^{e_1} \cdots (x - \xi_k)^{e_k}$ is a universal denominator of the homogeneous equation.

Inspection of the roots of the indicial polynomial in general does not suffice for predicting the pole orders of solutions of inhomogeneous equations. For example, the equation $x^2 f'(x) = 1$ has the rational solution $f(x) = -1/x$, while the indicial polynomial x only predicts constant solutions. In order to cover inhomogeneous equations, we need the following analog of Proposition 3.55 for finite points.

Proposition 3.60 *Let $p_0, \dots, p_r \in C[x]$, $p_r \neq 0$. Let $\xi \in C$ and let η be the indicial polynomial at ξ of the differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$. For a rational function $v \in C(x)$, let $\nu(v) \in \mathbb{Z}$ be the multiplicity of ξ as a root of v (taking negative integers when ξ is a pole and 0 when ξ is neither a pole nor a root). Let $d = \max_{i=0}^{r}(\nu(p_i) - i)$. Let $f \in C(x)$ and $n = \nu(f)$. If*

$$\nu(p_0 f + \cdots + p_r f^{(r)}) > n + d,$$

then $\eta(n) = 0$. □

Proof Write $p_i = \sum_{j=d+i}^{\infty} p_{i,j}(x-\xi)^j$ with $p_{i,j} = 0$ for all $j < 0$. By the choice of d, we have $\eta = \sum_{i=0}^{r} p_{i,d+i} x^{\underline{i}}$. If $f \in C(x)$ has the expansion $a_n(x-\xi)^n + a_{n+1}(x-\xi)^{n+1} + \cdots \in C((x-\xi))$, then $f^{(i)}$ has the expansion $a_n n^{\underline{i}}(x-\xi)^{n-i} + \cdots$ for $i = 0, \dots, r$, and then

$$\begin{aligned} p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) &= \sum_{i=0}^{r} p_i(a_n n^{\underline{i}}(x-\xi)^{n-i} + \cdots) \\ &= a_n \sum_{i=0}^{r} p_{i,d+i} n^{\underline{i}}(x-\xi)^{n+d} + \cdots . \end{aligned}$$

Applying ν to both sides and using the assumption, it follows that $\eta(n) = 0$. ■

Algorithm 3.61 (*Denominator bound*)
Input: *$p_0, \dots, p_r, g \in C[x]$ with $p_r \neq 0$. It is assumed that C is algebraically closed.*
Output: *A denominator bound for the differential equation $p_0 f + \cdots + p_r f^{(r)} = g$.*

Let $v = 1$.
for all roots ξ of p_r do
  Let η be the indicial polynomial η at ξ of the differential equation.
  Let $\xi_1, \dots, \xi_k$ be the integer roots of η.
  Let ν be the multiplicity of $x - \xi$ in g.
  Let $d = \max_{i=0}^{r}(\nu(p_i) - i)$, where $\nu(p_i)$ is the multiplicity of $x - \xi$ in p_i
  $v = (x-\xi)^{\max(-\xi_1, \dots, -\xi_k, d-\nu)} v$
Return v.

Theorem 3.62 *Algorithm 3.61 is correct.* □

Proof Let $f \in C(x)$ be such that $\sum_{i=0}^{r} p_i f^{(i)}(x) = g$, and let v be the output of Algorithm 3.61. We have to show that $vf \in C[x]$. Let $\xi \in C$ be arbitrary and let $e = \nu(vf)$, were ν refers to the multiplicity with respect to ξ. We have to show that $e \geq 0$. With η and d as in Proposition 3.60, we have $\nu(g) \leq \nu(f) + d$ or

$\eta(\nu(f)) = 0$, so $\nu(f) \geq \min\{\xi_1, \dots, \xi_k, \nu(g) - d\}$ if $\xi_1, \dots, \xi_k$ are the integer roots of η. In view of line 7, we have $e = \nu(vf) \geq 0$ if ξ is a root of p_r. If ξ is not a root of p_r, then $e \geq 0$ follows from the argument given in the paragraph following Definition 3.59. ■

Algorithm 3.61 also covers the case of homogeneous equations ($g = 0$) as well as parameterized equations. If $g = 0$, we can drop lines 5 and 6 and remove the argument $d - \nu$ from the maximum in line 7. If the maximum has no arguments at all because $g = 0$ and η has no integer roots ξ_i, the factor $x - \xi$ cannot occur in a denominator and we can take 0 as exponent. In the case of parameterized equations, if there are several inhomogeneous parts $g_1, \dots, g_m$, we have to set ν in line 5 to the minimum of the multiplicities of $x - \xi$ in the g_i.

Example 3.63

1. The differential equation

$$2(x-1)(x+2)f'''(x) + 2(10x^2 + 24x - 19)f''(x)$$
$$+ (37x^2 + 257x + 2)f'(x) + (296x + 283)f(x) = 0$$

has singularities at 1 and -2. The indicial polynomial at $\xi = 1$ is $\eta = 6x(x-1)(x+3)$, indicating a maximal pole order of 3 at $\xi = 1$. For $\xi = -2$ we get $\eta = -6x(x-1)(x+7)$, indicating a maximal pole order of 7 at $\xi = -2$. Hence $v = (x-1)^3(x+2)^7$ is a denominator bound for the equation.
In order to find the rational solutions, set $f = u/v$ for some new unknown function u into the equation. This gives the new equation

$$\begin{aligned}&2(x-1)^2(x+2)^2u'''(x) + 4(x-1)(x+1)(5x-8)(x+2)u''(x)\\&+ (37x^4 - 106x^3 - 75x^2 + 212x + 40)u'(x)\\&- 2(37x^3 - 123x^2 + 36x + 104)u(x) = 0.\end{aligned}$$

Its solution space in $C[x]$ is generated by $(x+1)^2$, so the solution space of the original equation in $C(x)$ is generated by $\frac{(x+1)^2}{(x-1)^3(x+2)^7}$.
2. Consider the parameterized equation

$$(x+1)f''(x) + (x+3)f'(x) + f(x) = c_0 + c_1 x.$$

The only singularity is $\xi = -1$, and the corresponding indicial polynomial is $\eta = x(x+1)$. Its integer roots are 0 and -1. The multiplicity of $x + 1$ in the inhomogeneous part is $\nu = 0$, and we have $d = -1$. Therefore, according to line 7 of Algorithm 3.61, a denominator bound for the equation is $(x+1)^1$.
In fact, the solution space in $C(x) \times C^2$ is generated by $(\frac{1}{x+1}, 0, 0)$, $(\frac{x}{x+1}, 1, 0)$, and $(\frac{x^2}{x+1}, 2, 2)$. □

It is not hard to construct examples where the denominator bound computed by Algorithm 3.61 is not tight. For example, the equation $2x(x+1)f'(x) + (9x + 10)f(x) = 0$ has the irrational solution $\sqrt{x+1}/x^5$, so its solution space in $C(x)$ is empty. Applying Algorithm 3.61 would give the denominator bound $v = x^5$. If we prefer an example which does have rational solutions, we can apply the closure properties algorithm for addition to the equation $2x(x+1)f'(x)+(9x+10)f(x) = 0$ and the equation $xf'(x) + f(x) = 0$, which has the rational solution $1/x$. The result is an equation of order two whose solution space is generated by $\sqrt{x+1}/x^5$ and $1/x$. Its solution space in $C(x)$ is generated by $1/x$, but Algorithm 3.61 would still return the suboptimal denominator bound x^5. In a sense, the algorithm recognizes that there is a certain solution with a pole of order 5 but does not detect that this solution is irrational.

On the other hand, there are also situations where Algorithm 3.61 does more than required. Observe that while the denominator v of any rational function u/v is by definition a polynomial, Definition 3.59 allows the denominator bound to be a rational function. Indeed, the exponent in line 7 of Algorithm 3.61 may well be negative. If this happens, the condition that vf is a polynomial for every rational solution f means that the denominator of v predicts certain factors of the numerator of rational solutions. More precisely, if v has a root ξ of multiplicity e, it means that ξ can be a pole of a rational function of order at most e, and if v has a pole ξ of multiplicity e, it means that every rational solution has at least a root of multiplicity e. While all potential poles of a rational function must necessarily be caught by the denominator bound, a rational solution typically has roots that are not predicted by the denominator bound. In fact, the denominator bound computed by Algorithm 3.61 predicts a root ξ of multiplicity $\geq e$ if and only if all power series solutions (rational or not) have a starting exponent $\geq e$.

Example 3.64 For the equation

$$\begin{aligned}12(x-1)(x+2)(x+1)^2 f''(x) + (19x^3 + 26x^2 + 29x + 214)(x+1)f'(x)\\ - (19x^3 + 7x^2 - 73x + 419)f(x) = 0\end{aligned}$$

we get the denominator bound $v = \frac{(x-1)^3(x+2)^2}{(x+1)^4}$, which says that the denominator of any rational solution divides $(x-1)^3(x+2)^2$ and the numerator of any rational solution is a multiple of $(x+1)^4$. Indeed, the solution space in $C(x)$ is generated by $\frac{(x+1)^5(x-2)}{(x-1)^3(x+2)}$. □

The example shows that sometimes a denominator bound can also predict some factors of the numerator, although in general they cannot predict all factors of the numerator. In the example, it is clear that the factor $x-2$ cannot be found, because 2 is not even a singularity of the equation. While poles of solutions must appear among the finitely many singularities of the equation, roots are not that restricted.

For example, every polynomial $x-\alpha \in C[x]$ is a solution of the differential equation $f''(x) = 0$, so in this case, every constant is a root of a solution.

Until now we have been assuming that the constant field C is algebraically closed. This assumption simplifies matters in theory, but not necessarily in practice. In the interest of efficiency, actual implementations should avoid calculations in fields that are larger than necessary. Ideally, we would prefer to stick to the smallest field that contains all coefficients which occur in the given equation. The question is then how to proceed if the leading coefficient p_r of the given equation contains irreducible factors of degree greater than 1, the roots of which belong to an extension field.

The technique discussed above for factors of degree 1 can be generalized to higher degree factors. The key observation is the following. If f is a rational function and v is an irreducible polynomial, we can write $f = v^\alpha u$ for some $\alpha \in \mathbb{Z}$ and some $u \in C(x)$ whose numerator and denominator are coprime with v. By induction on i, it can be easily shown that $f^{(i)} = \alpha^{\underline{i}} v^{\alpha-i}(v')^i u + v^{\alpha-i+1} w_i$ for some rational function w_i whose numerator and denominator are coprime with v. In this expression, $(v')^i$ is the ith power of the derivative of v.

Given some polynomials $p_0, \dots, p_r \in C[x]$, we can write them in the form $p_i = q_i v^{d+i}$ for some $q_0, \dots, q_r \in C(x)$ and some $d \in \mathbb{Z}$ to be fixed in a moment. We then have

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = \sum_{i=0}^{r}(q_i\alpha^{\underline{i}}(v')^i v^{\alpha+d}u(x) + q_i v^{\alpha+1+d} w_i(x)).$$

Therefore, in order for $p_0 f + \cdots + p_r f^{(r)}$ to be zero, or, more generally, to contain v with a greater power than $\alpha+d$, we must have $\sum_{i=0}^{r}(q_i(v')^i \bmod v)\alpha^{\underline{i}} = 0$. Since v is irreducible, we have $\gcd(v, v') = 1$, so we have obtained a nonzero polynomial constraint on α as soon as there is at least one i for which $v \nmid q_i$, which can be ensured by a proper choice of d. This reasoning motivates the following definition.

Definition 3.65 Let $p_0, \dots, p_r \in C[x]$ with $p_r \neq 0$. Let $v \in C[x]$ be irreducible. For a rational function $h \in C(x)$, let $\nu_v(h)$ be the unique integer such that v divides neither the numerator nor the denominator of $v^{-\nu_v(h)}h$. Let $d = \min_{i=0}^{r}(\nu_v(p_i) - i)$, and let $q_i \in C[x]$ be such that $p_i = q_i v^{d+i}$ for $i = 0, \dots, r$. Define $H = \sum_{i=0}^{r}((v')^i q_i \bmod v)y^{\underline{i}} \in C[x, y]$ and let η be the greatest common divisor in $C[y]$ of the coefficients of H with respect to x. Then η is called the indicial polynomial of the equation $p_0 f + \cdots + p_r f^{(r)} = 0$ with respect to v. □

Example 3.66 For the differential equation

$$(x^2+1)^2 f''(x) + 6(x+1)(x^2+1)f'(x) - 6(x^2-6x-1)f(x) = 0$$

and the polynomial $v = x^2 + 1$, we have $d = 0$ and $q_0 = -6(x^2 - 6x - 1)$, $q_1 = 6(x+1)$, $q_2 = 1$. With these polynomials and $v' = 2x$ we get the auxiliary polynomial

$$\begin{aligned} H &= 12(1+3x) + 12(x-1)y + (-4)y(y-1) \\ &= -4(y+3)(y-1) + 12(y+3)x \in C[x, y] \end{aligned}$$

and finally $\eta = \gcd(-4(y+3)(y-1), 12(y+3)) = y+3 \in C[y]$ with respect to v. □

Proposition 3.60 and Algorithm 3.61 admit straightforward generalizations to irreducible polynomials of higher degree. Instead of looping over the roots of p_r, which may belong to an algebraic extension of C, we should loop over the irreducible factors of p_r. In line 3 we use the indicial polynomial defined in Definition 3.65, and in lines 5–7, we use the irreducible factor instead of $x - \xi$. The algorithm then returns an element of $C(x)$ which is a valid denominator bound.

Example 3.67 Continuing the previous example, we obtain the denominator bound $v = (x^2 + 1)^3$. In fact, $1/(x^2 + 1)^3$ turns out to be a rational solution. □

We can consider rational functions as "closed form" expressions. If a certain D-finite power series $f \in C[[x]]$ is specified through a differential equation and initial values, we can decide whether f is the series expansion of a rational function by first finding a basis of the solution space of the differential equation in $C(x)$, then expanding the basis elements as power series (or Laurent series), and then checking whether some C-linear combination is equal to f. If this is the case, we have found a rational closed form for f, and if not, we have proven that no such closed form exists.

Example 3.68 Consider the power series $f(x) = 1-5x+3x^2-15x^3+\cdots \in C[[x]]$ satisfying the differential equation

$$(x-1)^2(x+1)^2 f'''(x)+16(x-1)x(x+1)f''(x)+6(11x^2-3)f'(x)+60xf(x) = 0.$$

The solution space of this equation in $C(x)$ is generated by $\frac{1}{(1-x)^2(1+x)^3}$ and $\frac{1}{(1-x)^3(1+x)^2}$. Therefore, if f admits a rational closed form, it must be a C-linear combination of these two solutions. Equating the first two coefficients of

$$\begin{aligned} & f(x) - \alpha \frac{1}{(1-x)^2(1+x)^3} - \beta \frac{1}{(1-x)^3(1+x)^2} \\ & = (1-\alpha-\beta) + (-5+\alpha-\beta)x + (3-3\alpha-3\beta)x^2 + \cdots \end{aligned}$$

to zero gives a linear system for (α, β) with the unique solution $(\alpha, \beta) = (3, -2)$. Since 0 is an ordinary point of the differential equation, we know that the only power series solution of the form $0+0x+\cdots$ is the zero series. Therefore, we can conclude $f(x) = \frac{3}{(1-x)^2(1+x)^3} - \frac{2}{(1-x)^3(1+x)^2} = \frac{5x-1}{(1-x)^3(1+x)^3}$. □

Typically, a differential equation does not have any nonzero solutions in $C(x)$, and even if it does, the chances that a particular series solution matches the expansion of a rational solution are rather low (unless, of course, if the dimension of the solution space in $C(x)$ matches the order of the equation). Whenever the defining equation of f has rational solutions but f itself is not rational, it may be possible to view f as a sum $g+q$ where q is a rational function and g is a D-finite power series which satisfies a differential equation of lower order. If $q_1, \dots, q_m$ form a basis of the solution space in $C(x)$, then such a decomposition of f can be found by making an ansatz $g = f - \alpha_1 q_1 - \cdots - \alpha_m q_m$ with undetermined coefficients $\alpha_1, \dots, \alpha_m$ and guessing a lower order differential equation for g using the techniques of Sect. 1.5. The guessing procedure will lead to an overdetermined linear system whose coefficients involve the undetermined α_i. By computing suitable determinants, we get a system of polynomial equations for the α_i, the solutions of which indicate the values for which there exists a guessed equation. Using closure properties, we can then prove that the guessed equation is indeed correct.

Example 3.69 Consider the power series $f(x) = \frac{9}{2}x - \frac{9}{8}x^2 + \frac{27}{4}x^3 + \cdots \in C[[x]]$ satisfying the differential equation

$$2(x-1)(x+2)f''(x) + (3x^2+17x-2)f'(x) + (12x+19)f(x) = 0.$$

The solution space in $C(x)$ of this differential equation is generated by $\frac{x+1}{(1-x)^2(x+2)^3} \in C(x)$. Its series expansion $\frac{1}{8} + \frac{3}{16}x + \frac{1}{4}x^2 + \cdots$ is obviously not a constant multiple of f, which proves that f does not admit a rational closed form.

Let us see whether $f(x) = g(x) + \alpha\frac{x+1}{(1-x)^2(x+2)^3}$ for some $\alpha \in C$ and some g which satisfies a differential equation of order 1. We have

$$\begin{aligned} g(x) &= f(x) - \alpha\frac{x+1}{(1-x)^2(x+2)^3} \\ &= -\frac{\alpha}{8} + \left(\frac{9}{2} - \frac{3\alpha}{16}\right)x + \left(-\frac{9}{8} - \frac{\alpha}{4}\right)x^2 + \left(\frac{27}{4} - \frac{11\alpha}{32}\right)x^3 + \cdots \end{aligned}$$

For a specific choice d, consider the ansatz $\sum_{i=0}^{1}\sum_{j=0}^{d} p_{i,j}x^j g^{(i)}(x) = 0$ for an equation for g. There will be no solution for $d = 0, 1, 2, 3$, so let us skip these cases and directly consider the case $d = 4$. We then have ten unknowns $p_{i,j}$, and by matching sufficiently many terms of g to the ansatz, we can produce a system of ten linear equations for them:

$$\begin{pmatrix} -\frac{\alpha}{8} & 0 & 0 & 0 & 0 & \frac{9}{2}-\frac{3\alpha}{16} & 0 & 0 & 0 & 0 \\ \frac{9}{2}-\frac{3\alpha}{16} & -\frac{\alpha}{8} & 0 & 0 & 0 & -\frac{9}{4}-\frac{\alpha}{2} & \frac{9}{2}-\frac{3\alpha}{16} & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} p_{0,0} \\ p_{0,1} \\ \vdots \\ p_{1,0} \\ p_{1,1} \\ \vdots \end{pmatrix} = 0.$$

The determinant of the matrix in this system is a polynomial in α of degree 8 which splits into a nice factor of degree 1 and an ugly factor of degree 7. The nice factor is $\alpha - 8$, suggesting that $\alpha = 8$ is a good choice. For this choice, the system has a solution space of dimension one which gives rise to the guessed equation

$$(6x^4 + 22x^3 - 4x^2 - 40x + 16)g'(x) + (9x^4 + 51x^3 + 52x^2 - 76x + 48)g(x) = 0$$

for g. Since the equation has first order, we can find its solutions by separating variables. It turns out that $g(x) = \frac{3x^2+8x-4}{(x-1)^2(x+2)^3}\exp(-3x/2)$ is a solution of the guessed equation, and it is easy to check that this expression is also a solution of the original equation for f. Therefore, we have $f(x) = \beta\frac{3x^2+8x-4}{(x-1)^2(x+2)^3}\exp(-3x/2) + 8\frac{x+1}{(1-x)^2(x+2)^3}$ for some $\beta \in C$, and by comparing the first term of the expansion on both sides, we finally find that $\beta = 9$. □

Exercises

1*.** Consider a differential equation $\sum_{i=0}^{r} p_i f^{(i)} = 0$ with $p_0, \ldots, p_r \in C[x]$. Let $\eta_\infty \in C[x]$ be its indicial polynomial at infinity (in the sense of Definition 3.48). Now apply a change of variables $\tilde{x} = 1/x$ to the equation and let $\tilde{\eta}_0 \in C[x]$ be the indicial polynomial of the resulting equation at 0 (in the sense of Definition 3.34). Show that $\eta_\infty(x) = \tilde{\eta}_0(-x)$, and explain why there is a sign change in the argument.

Hint: You may want to reuse the formulas proven in Exercise 1 of Sect. 3.2.

2*. In a computer algebra system of your choice, write a program which finds a basis of the solution space in $C[x]$ of any given homogeneous differential equation with polynomial coefficients.

3. Find all polynomial solutions of the following equations:

a. $f^{(5)}(x) = 0$;

b. $xf^{(4)}(x) + xf'''(x) + xf''(x) + xf'(x) - 8f(x) = 0$;

c. $x^4 f^{(4)}(x) - 95x^3 f'''(x) - 96x^2 f''(x) - 97xf'(x) - 99f(x) = 0$;

d. $2(x-1)(x+4)f'''(x) + (x^2-30x-41)f''(x) - 18(x-7)f'(x) + 88f(x) = 0$.

4. Show that there are no $\alpha, \beta, \gamma, \delta, \epsilon \in C$ such that the equation

$$(x+\alpha)f(x) - (\beta x + \gamma)f'(x) - (\delta x + \epsilon)f''(x) = 0$$

has a nonzero polynomial solution.

5. Show that the cost of computing the associated recurrence in line 6 of Algorithm 3.51 is bounded by $O(r^2(r+d))$ operations in C.

6. Find all differential equations of order ≤ 2 and degree ≤ 2 which have the rational function $\frac{x^3-5x^2+5x-2}{x-1}$ as a solution.

7. According to Proposition 3.49, the largest integer root of the indicial polynomial at infinity is an upper bound for the degree of the polynomial solutions of a homogeneous equation. Is the smallest integer root of the indicial polynomial at infinity a lower bound for the degree of the polynomial solutions?

8*. Suppose a differential equation of order r and degree d has a polynomial solution of the form $p + x^n q$ for some $n > r + d + \deg_x p$ and some $p, q \in C[x]$. Show that $p - x^n q$ is also a solution of the equation.

9. Prove or disprove: A differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ has a nonzero constant solution if and only if $p_0 = 0$.

10*. For each of the following equations, find all constants $\alpha \in C$ for which the equation has a nonzero polynomial solution.

a. $2f''(x) - xf'(x) + \alpha f(x) = 0$;
b. $18\alpha f''(x) - (\alpha + x)^2 f'(x) + 2xf(x) = 0$;
c. $f''(x) - (\alpha + x)f'(x) + 3f(x) = 0$.

11. Find all rational solutions of the following equations:

a. $x^3 f^{(4)}(x) + 12x^2 f'''(x) + 36xf''(x) + 24f'(x) = 0$;
b. $(x-1)(x+2)f''(x) + (7x+5)f'(x) + 8f(x) = 0$;
c. $(x-1)(x+2)f''(x) + (3x^2+4x-13)f'(x) - 2(3x+14)f(x) = 0$;
d. $x(x+1)f'''(x) - 3(2x^2-1)f''(x) - 6(4x+1)f'(x) - 12f(x) = 0$;
e. $(x-1)^3(x+1)^3 f'''(x) + 12(5x^3+5x^2+5x+1)f(x) = 0$.

12. Find all solutions in $C(x) \times C^2$ of the following parameterized equations:

a. $(x+1)f'(x) + (x+2)f(x) = c_1 + c_2 x$;
b. $(x+1)f''(x) - (x+1)f'(x) + (x+1)f(x) = c_1 x + c_2 x^2$;
c. $3(x+1)^2 f''(x) - (3x-23)(x+1)f'(x) - 3(x-6)(x+3)f(x) = c_1 x + c_2 x^2$;
d. $(x+1)^2 f'(x) - 2(x+1)f(x) = c_1 x + c_2 x^5$;
e. $(x+1)^2 f''(x) + 2(x+1)f'(x) + x(x+1)f(x) = c_1(x+\sqrt{x}) + c_2(x-2\sqrt{x})$.

13. Find all rational solutions of the following differential equation:

$$(x+1)(x+2)f''(x) + (\sqrt{x}+1)(x+2)(x-\sqrt{x}+2)f'(x) + \sqrt{x}f(x) = 0.$$

14. What are the possible dimensions that the solutions space of a parameterized equation $p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = c_1 g_1(x) + \cdots + c_m g_m(x)$ in $C(x) \times C^m$ can have?

15*.** Continuing Exercise 4, show that there are no $\alpha, \beta, \gamma, \delta, \epsilon \in C$ such that the equation

$$(x+\alpha)f(x) - (\beta x+\gamma)f'(x) - (\delta x+\epsilon)f''(x) = 0$$

has a nonzero rational solution.

16. Find a rational closed form expression for the power series $f \in C[[x]]$ defined by

$$3(x-1)(2x+1)f'''(x) - (2x-11)(4x-1)f''(x) - 8(4x-7)f'(x) - 16f(x) = 0$$

and the initial values $f(x) = 1 + 9x - 13x^2 + 43x^3 + \cdots$.

17. Prove or disprove: The power series solution $f(x) = x + 2x^2 + 2x^3 + 4x^4 + 3x^5 + \cdots \in C[x]$ of the differential equation

$$(x-1)^2(x+1)^2 f'''(x) + 12(x-1)x(x+1)f''(x) + 12(3x^2-1)f'(x) + 24xf(x) = 0$$

admits a rational closed form.

18. Consider the series $f(x) = 2 + \frac{9}{4}x - \frac{65}{8}x^2 + \frac{355}{24}x^3 + \cdots \in C[[x]]$ defined by the differential equation

$$\begin{aligned}
&4(x+1)^2(x+2)^2(x+3)f'''(x)\\
&\quad + (x+1)(x+2)(9x^3+78x^2+219x+182)f''(x)\\
&\quad + (29x^4+264x^3+871x^2+1208x+588)f'(x)\\
&\quad + (11x^3+99x^2+236x+166)f(x) = 0.
\end{aligned}$$

Show that $f = g + q$ for some $q \in C(x)$ and a D-finite power series g satisfying a differential equation of order 2 and degree 2.

19. Prove or disprove:

a. If $\xi \in C$ is an apparent singularity, it will not be a root of the denominator bound computed by Algorithm 3.61.

b. If $\xi \in C$ is a singularity but not a root of the denominator bound computed by Algorithm 3.61, then ξ is an apparent singularity.

20. Construct a differential equation whose solution space in $C(x)$ is generated by $\frac{x+1}{x-1}$ and $\frac{x-1}{x+1}$.

21.** Let C_{sub} be a subfield of C and consider a differential equation with coefficients in $C_{\text{sub}}[x]$. Show that the solution space of this equation in $C(x)$ has a basis whose elements belong to $C_{\text{sub}}(x)$.

22. Design an algorithm which for a given differential equation with coefficients in $C[x]$ finds a basis of its solution space in $\bigcup_{v\in\mathbb{N}\setminus\{0\}} C(x^{1/v})$.

23****.** Design an algorithm which for a given differential equation with coefficients in $C[\exp(x)]$ finds a basis of its solution space in $C[\exp(x)]$.

24***.** Find all $g \in C(x)$ such that $\sqrt{g}$ is a solution of

$$(x-1)(x+1)f''(x) - (x^2 - 2x - 2)f'(x) + (x-1)f(x) = 0.$$

Hint: Construct an equation for g and find its rational solutions.

25. With the notation of Definition 3.65, suppose that H has an irreducible factor which involves both x and y. Show that at a root $\xi \in \bar{C}$ of v, the differential equation has a generalized series solution involving an exponential part.

26. Can we replace "irreducible" by "squarefree" in Definition 3.65?

27. (Marc Mezzarobba) Show that the degree of the indicial polynomial as defined in Definition 3.65 can be less than the order of the differential equation even at a regular singularity.

References

The basic ideas of bounding the degree of a polynomial solution and solving a linear system, and of bounding the denominator of a rational solution in order to reduce the problem to finding polynomial solutions are too classic to be able to name an inventor of these ideas. Already in 1833, Liouville [312] knew how to find polynomial solutions. Efficient algorithms based on series expansions were introduced by Abramov and Kvashenko [12]. The idea to quickly check the existence of polynomials solutions without actually computing them appears in a paper of Bostan, Cluzeau, and Salvy [80]. Parameterized equations with several inhomogeneous parts arise in integration algorithms, as we shall see in Chap. 5.

Generalizing the setting studied in this section, we can consider a linear differential equation with coefficients in some differential field K, and we can ask for the solution space in K of this equation. Finding rational solutions as discussed in this section amounts to the special case $K = C(x)$ with the usual derivation. The ideas can be extended to more complicated differential fields. Exercises 23 and 24 go in this direction. Singer [408] and Bronstein [111] propose general algorithms for cases where the field K may contain certain transcendental functions. It is a more difficult problem to find closed form solutions that do not belong to the differential field K in which the coefficients of the equation live, but to some larger field. This situation is the topic of the next section.

3.6 Hyperexponential and d'Alembertian Solutions

In Example 3.69, we had a differential equation with a rational solution and another solution that could be expressed as a solution of a first order differential equation. Equations of order one can always be solved in terms of elementary functions by separating variables. Starting from an equation $p_0(x)f(x) + p_1(x)f'(x) = 0$, the classical advice is to bring f and f' to one side and p_0, p_1 to the other side, then integrate, and then apply exp:

$$\begin{aligned} p_0(x)f(x) + p_1(x)f'(x) = 0&, \\ \frac{f'(x)}{f(x)} &= -\frac{p_0(x)}{p_1(x)}, \\ \log f(x) &= -\int \frac{p_0(x)}{p_1(x)}, \\ f(x) &= \exp(-\int \frac{p_0(x)}{p_1(x)}). \end{aligned}$$

If C is algebraically closed, we can express the indefinite integral on the right hand side as the sum of a rational function and a linear combination of logarithms of polynomials, i.e., $-\int \frac{p_0(x)}{p_1(x)} = g(x) + \sum_{i=1}^{m} \alpha_i \log(h_i(x))$ for some $g \in C(x)$, $\alpha_i \in C$, and $h_i \in C[x]$. This can be seen easily by considering the partial fraction decomposition of the integrand and integrating term by term. If C is not algebraically closed, there still exist $g \in C(x)$, $\alpha_i \in \bar{C}$ and $h_i \in C(\alpha_i)[x]$ with $-\int \frac{p_0(x)}{p_1(x)} = g(x) + \sum_{i=1}^{m} \alpha_i \log(h_i(x))$, as will be shown in Sect. 5.1. In any case, by applying the exponential function, we find that the general solution of a first order differential equation $p_0(x)f(x) + p_1(x)f'(x) = 0$ has the form

$$f(x) = \exp(g(x)) \prod_{i=1}^{m} h_i(x)^{\alpha_i}.$$

Such expressions are called *hyperexponential functions.* They need not be functions in the strict sense of the word but can also be certain algebraic objects that are just called functions, similar like rational functions. If all the α_i are integers, then $f(x)$ is the product of an exponential function and a rational function. In this case, the rational function is called the *shell* and the exponential function is called the *kernel* of $f(x)$. In general, the α_i need not be integers, but it can nevertheless be useful to think of the hyperexponential function as consisting of a rational part, called the shell, and a transcendental part, called the kernel. With such a factorization in mind, we will develop an algorithm that finds hyperexponential solutions of differential equations by first finding potential kernels and then constructing the corresponding shells. The decomposition of hyperexponential functions into shells and kernels is also useful in the context of integration algorithms discussed in Chap. 5. The precise definition of shell and kernel for arbitrary hyperexponential functions is given in the definition below. In this definition, we also extend the concepts *exponential* and *hyperexponential* to arbitrary differential fields.

Definition 3.70 (See Definition 2.72 for the shift case) Let K be a differential field and E be a differential field extension of K. Let $y \in E \setminus \{0\}$.

1. y is called *exponential* over K if there exists a $g \in K$ such that $y'/y = g'$.
2. y is called *hyperexponential* over K if there exists a $g \in K$ such that $y'/y = g$.

Suppose now that $K = C(x)$, that y is hyperexponential, and let $u, v \in C[x]$ be such that $y'/y = u/v$.

3. y is called a *kernel* if $\gcd(u - iv', v) = 1$ for all $i \in \mathbb{Z}$.
4. $s \in C(x)$ is called a *shell* for y if y/s is a kernel. We then say that y/s is a kernel of y.

□

If the ground field K is not specified, we mean $K = C(x)$ (together with the usual derivation). For this case, we have derived a general expression for the hyperexponential functions above. Note that in particular, every rational function is hyperexponential.

Example 3.71

1. e^{e^x} is exponential over $C(e^x)$ but not over $C(x)$.
2. x is hyperexponential over $C(x)$, but not exponential, because $x'/x = 1/x$ is not integrable in $C(x)$. More generally, every element of K is hyperexponential over K.
3. $x^{\sqrt{2}}$ is hyperexponential over $\mathbb{Q}(\sqrt{2})(x)$, but not over $\mathbb{Q}(x)$.
4. $y = \sqrt{x}$ is a kernel, because $y'/y = 1/(2x) = u/v$ with $\gcd(u - iv', v) = \gcd(1 - 2i, 2x) = 1$ for all $i \in \mathbb{Z}$. Also $y = x\sqrt{x}$ is a kernel, because in this case we have $y'/y = 3/(2x) = u/v$ with $\gcd(u - iv', v) = \gcd(3 - 2i, 2x) = 1$ for all $i \in \mathbb{Z}$.
5. $y = (x + 1)\sqrt{x}$ is not a kernel, because for $y'/y = \frac{1+3x}{2x(x+1)} = u/v$ we have $\gcd(u + v', v) = \gcd(-1 - x, 2x(x + 1)) = x + 1 \neq 1$. Since $\sqrt{x}$ is a kernel, $y/\sqrt{x} = x + 1$ is a shell for y. Furthermore, since also $x\sqrt{x}$ is a kernel, also $\frac{y}{x\sqrt{x}} = \frac{x+1}{x}$ is a shell for y. □

If $y_1, y_2 \in E$ are hyperexponential over K, their product is also hyperexponential (Exercise 1). Furthermore, if $y \in E$ is hyperexponential, so are y' and $1/y$. However, the sum of two hyperexponential functions may not be hyperexponential. For example, 1 and $\exp(x)$ are both hyperexponential, but their sum $1+\exp(x)$ is not. In general, the sum of two hyperexponential functions y_1, y_2 is again hyperexponential if and only if their quotient y_1/y_2 is a rational function (Exercise 6). In this case, y_1 and y_2 are called *similar*. Similarity is an equivalence relation on the set of hyperexponential functions. Each equivalence class together with zero forms a $C(x)$-vector space which is closed under derivation.

In particular, for any $p_0, \ldots, p_r \in C[x]$ and a hyperexponential function y, we have that $p_0 y + p_1 y' + \cdots + p_r y^{(r)}$ is either zero or similar to y. Because of this observation, it is easy to find hyperexponential solutions of inhomogeneous equations $p_0 y + p_1 y' + \cdots + p_r y^{(r)} = g$ with a hyperexponential right hand side g. It suffices to make an ansatz $y = rg$ for an unknown rational function r, plug it into the left hand side and divide the equation by g. This gives an inhomogeneous equation for the unknown rational function r, which can be solved using the techniques of the previous section.

Example 3.72

1. In order to find a hyperexponential closed form for the integral $\int \exp(x^2)dx$, we have to solve the differential equation $y'(x) = \exp(x^2)$. Setting $y(x) = r(x)\exp(x^2)$ for an unknown rational function r, the differential equation translates into $r'(x)\exp(x^2) + r(x)\exp(x^2)2x = \exp(x^2)$, i.e., $r'(x) + 2xr(x) = 1$. Since this equation has no rational solution, the integral has no hyperexponential closed form.
2. If we proceed along the same lines for the integral $\int (x^2 + 4x + 2)\exp(\frac{x^2}{x+1})dx$, we obtain the differential equation

$$(x^2+4x+2)(x+1)^2 r'(x) + (x+2)(x^3+6x^2+6x+2)r(x) = (x^2+4x+2)(x+1)^2,$$

which has the rational solution $r = \frac{(x+1)^2}{x^2+4x+2}$. Therefore,

$$\int (x^2 + 4x + 2)\exp(\frac{x^2}{x+1})dx = (x + 1)^2 \exp(\frac{x^2}{x+1}).$$

□

It is more difficult to find hyperexponential solutions of homogeneous equations, because the 0 on the right hand side gives no clue about the similarity classes in which solutions may exist. Clearly, for any given hyperexponential function h, we can determine all rational functions r such that rh is a solution of a given homogeneous equation in the same way as we did in the previous example for an inhomogeneous equation. It is therefore sufficient to determine, for a given homogeneous equation, a finite set of hyperexponential functions $h_1, \ldots, h_m$ such that every hyperexponential solution of the equation must be a rational multiple of one of them.

As we have noticed above, the set of hyperexponential functions is not closed under addition, so in particular it does not form a ring. The set of hyperexponential solutions of a given equation is therefore in general not a vector space and it is meaningless to speak about its dimension. Nevertheless, the number of pairwise non-similar hyperexponential solutions cannot exceed the order of the equation. For, if $h_1, \ldots, h_m$ are such solutions, we can consider the differential ring $C(x)[h_1, \ldots, h_m]$, to which Theorem 3.22 is applicable. The solution space of the equation in this ring is bounded by the order of the equation, and it must contain the functions $h_1, \dots, h_m$, which are linearly independent over C (even over $C(x)$). So m is also bounded by the order.

If we write a differential equation in terms of operators, the search for a hyperexponential solution is equivalent to the search for a first order right hand factor.

Lemma 3.73 *(See Lemma 2.78 for the shift case) Consider a differential operator $L = p_0 + p_1 D + \cdots + p_r D^r \in C(x)[D]$. Then L has a hyperexponential solution y with $D(y)/y = u/v$ if and only if L has a first order right factor $u - vD$.*

Proof "$\Leftarrow$" Clearly y is a solution of $u - vD$. If $L = Q(u - vD)$ for some operator $Q \in C(x)[D]$, then $L \cdot y = Q(u - vD) \cdot y = Q \cdot \big((u - vD) \cdot y\big) = Q \cdot 0 = 0$, so y is a solution of L.

"$\Rightarrow$" The operator L has $u - vD$ as a right factor if and only if every operator $L - Q(u - vD)$, for some $Q \in C(x)[D]$ has $u - vD$ as a right factor.

Induction on the order r: The case $r = 0$ cannot occur because L is supposed to have a hyperexponential solution, and operators of order $r = 0$ have no nonzero solutions. For $r = 1$, consider $L + \frac{p_1}{v}(u - vD) = p_0 + \frac{p_1 u}{v}$. Since y must be a solution of this operator, we must have $p_0 + \frac{p_1 u}{v} = 0$, so $-p_0/p_1 = u/v$. It follows that $L = p_0 + p_1 D$ is a left multiple of $u - vD$. Suppose now the claim holds for operators of order $\leq r - 1$. Then for an operator $L = p_0 + \cdots + p_r D^r$ of order r, consider the operator $L + \frac{p_r}{v} D^{r-1}(u - vD)$. This operator has order $\leq r - 1$ and it has y as solution. By the induction hypothesis, it has $u - vD$ as a right factor. Consequently, so does L. ∎

In order to find all hyperexponential solutions of a given differential equation, we will apply the local-to-global approach. This means that the hyperexponential functions ("global solutions") are obtained by inspection of the generalized series solutions ("local solutions") at the singularities. The lemma above justifies this approach: if a given differential equation has a hyperexponential solution y with $y'/y = u/v$, then the corresponding operator has $u - vD$ as right factor, so any generalized series solution of the right factor must also be a generalized series solution of the differential equation. Stated less formally, if a hyperexponential expression $\exp(g(x)) \prod_{i=1}^{m} h_i(x)^{\alpha_i}$ satisfies a certain differential equation, then so must its series expansion at any point $\xi \in \bar{C} \cup \{\infty\}$.

Note that the series expansions of hyperexponential expressions match the form of the generalized series discussed in Sect. 3.4. For example, for the function

$$f(x) = \exp\left(\frac{x^2}{(x+1)(x-1)^3}\right)(x+1)^{1/2}(x-1)^3 x^{-5},$$

we have the expansions

$$-x^{-5} + \tfrac{5}{2}x^{-4} - \tfrac{3}{8}x^{-3} - \tfrac{23}{16}x^{-2} + \cdots \qquad \text{at } 0,$$
$$\sqrt{2}\exp\big(\tfrac{1}{2(x-1)^3} + \tfrac{3}{4(x-1)^2} + \tfrac{1}{8(x-1)} - \tfrac{1}{16}\big)(x-1)^3\big(1 - \tfrac{151}{32}(x-1) + \cdots\big) \quad \text{at } 1,$$
$$8\exp\big(-\tfrac{1}{8(x+1)} + \tfrac{1}{16}\big)(x+1)^{1/2}\big(1 + \tfrac{57}{16}(x+1) + \tfrac{4353}{512}(x+1)^2 + \cdots\big) \qquad \text{at} -1,$$
$$x^{-3/2}\big(1 - \tfrac{5}{2}x^{-1} + \tfrac{19}{8}x^{-2} + \tfrac{7}{16}x^{-3} + \cdots\big) \qquad \text{at } \infty.$$

At every other point, the expansion is simply a power series. The exponential part of f is exactly the product of the exponential parts of all of the series solutions, because

$$\frac{x^2}{(x+1)(x-1)^3} = \frac{1}{2(x-1)^3} + \frac{3}{4(x-1)^2} + \frac{1}{8(x-1)} - \frac{1}{8(x+1)}.$$

This must be the case because an exponential function $\exp(g(x))$ admits a power series expansion at ξ if and only if the rational function g has no pole at ξ. We can take advantage of the fact that a differential equation has at most finitely many singularities, and that at each singularity, the generalized series solutions can only have finitely many distinct exponential parts. This gives us finitely many candidates for the exponential parts of a potential hyperexponential solution.

For each candidate $g(x)$, we can make a change of variables $f(x) = \exp(g(x))\tilde{f}(x)$ and construct a differential equation for a new unknown function $\tilde{f}$. If the original equation has a solution $\exp(g(x))\prod_{i=1}^m h_i(x)^{\alpha_i}$, the new equation will have a solution $\prod_{i=1}^m h_i(x)^{\alpha_i}$. If we could assume that the exponents α_i are integers, this would just be a rational function, and we could find it with the techniques of the previous section.

In general, the α_i are not integers, but whenever they are not, the roots of the corresponding $h_i(x)$ must be singularities of the equation, and we can take the finitely many distinct exponents appearing in the generalized series solutions at these roots as candidates. The generalized series will even tell us with which exponential parts a particular exponent candidate can occur in combination. Also, whenever two exponent candidates differ by an integer, it suffices to consider one of them, because as soon as we have $g \in C(x)$ and $\alpha_1, \ldots, \alpha_m \in C$ such that for some (unknown) integers $e_1, \ldots, e_m \in \mathbb{Z}$ there is a hyperexponential solution $\exp(g(x))\prod_{i=1}^m h_i(x)^{\alpha_i + e_i}$ then making a change of variables $f(x) = \exp(g(x))\prod_{i=1}^m h_i(x)^{\alpha_i}\tilde{f}(x)$ reduces the problem to finding a rational function solution $\tilde{f}$.

To simplify the discussion, let us say that the pair $(u, \alpha + \mathbb{Z})$ is the *type* of a generalized series $\exp(u(1/\bar{x}))\bar{x}^\alpha a(\bar{x}, \log(x))$, where $\bar{x} = x - \xi$ or $\bar{x} = x^{-1}$. Altogether, we have the following algorithm for finding all hyperexponential solutions of a given differential equation.

Algorithm 3.74 (*See Algorithm 2.82 for the shift case*)
Input: $p_0, \ldots, p_r \in C[x]$ *with* $p_r \neq 0$. *It is assumed that* C *is algebraically closed.*

Output: *A set S of hyperexponential functions y with $p_0 y + \cdots + p_r y^{(r)} = 0$ such that every other hyperexponential solution of this differential equation is a C-linear combination of elements of S.*

1 *Let $\xi_0 = \infty$ and let $\xi_1, \ldots, \xi_k \in C$ be the roots of p_r.*
2 *for $i = 0, \ldots, k$ do*
3   *Determine a finite set $E_i \subseteq C[x] \times C/\mathbb{Z}$ such that for every generalized series solution at ξ_i of type $(u, \alpha + \mathbb{Z})$ we have $(u, \alpha + \mathbb{Z}) \in E_i$.*
4 *Set $H = \emptyset$.*
5 *for all tuples $((u_0, \alpha_0 + \mathbb{Z}), \ldots, (u_k, \alpha_k + \mathbb{Z})) \in E_0 \times \cdots \times E_k$ do*
6   *if $\sum_{i=0}^k \alpha_i \in \mathbb{Z}$ then*
7   *Set $q = \exp(u_0(x)) \prod_{i=1}^k \exp(u_i(1/(x - \xi_i)))(x - \xi_i)^{\alpha_i}$.*
8   *Apply the change of variables $y = q\tilde{y}$ to the input differential equation and find a basis $\{b_1, \ldots, b_\ell\} \subseteq C(x)$ of the space of all the rational solutions $\tilde{y}$ of the resulting equation.*
9   *$H = H \cup \{q b_j : j = 1, \ldots, \ell\}$.*
10 *Return H.*

Theorem 3.75 *Algorithm 3.74 is correct.* □

Proof It is clear by construction that every element of the output set is a hyperexponential solution of the input equation. Conversely, suppose that y is any hyperexponential solution of the input equation. We have to show that it is a C-linear combination of the elements of the output set H.

In view of Lemma 3.73, the first order equation defining y must be a right factor of the input equation. Every generalized series solution of this first order equation is therefore also a solution of the input equation. Their exponential parts $\exp(u(\bar{x}))\bar{x}^\alpha$ must therefore appear among those collected in line 3. It is legitimate that line 3 only considers singular points, because we cannot have a nontrivial exponential part at an ordinary point. Altogether, it follows that in (at least) one iteration of the loop starting in line 5 we have that the hyperexponential terms $q = \exp(u_0(x)) \prod_{i=1}^k \exp(u_i(1/(x - \xi_i)))(x - \xi_i)^{\alpha_i}$ are such that $\tilde{y} = y/q$ is a rational function. If we pass the condition of line 6, the rational function $\tilde{y}$ will be a C-linear combination of the $b_1, \ldots, b_\ell$ computed in line 8, so y will be a C-linear combination of the terms added to H in line 9.

To see that the filter of line 6 is justified, observe that the expansion of $\prod_{i=1}^k (x - \xi_i)^{\alpha_i}$ at infinity has the form $x^{\sum_{i=1}^k \alpha_i} + \cdots = (\frac{1}{x})^{-\sum_{i=1}^k \alpha_i} + \cdots$, so we must have $\alpha_0 + \mathbb{Z} = -\sum_{i=1}^k \alpha_i + \mathbb{Z}$. ■

Example 3.76

1. The differential equation

$$16x^3 f''(x) + 32x^2 f'(x) + (-x^2 + 4x - 3) f(x) = 0$$

has no hyperexponential solutions, because its only generalized series solutions at 0 are

$$\mathrm{e}^{\sqrt{3/(4x)}}x^{-1/4}\Big(1+\frac{1}{4\sqrt{3}}x^{1/2}+\frac{3}{32}x+\cdots\Big)\quad\text{and}$$
$$\mathrm{e}^{-\sqrt{3/(4x)}}x^{-1/4}\Big(1-\frac{1}{4\sqrt{3}}x^{1/2}+\frac{3}{32}x+\cdots\Big),$$

and the kernel of a hyperexponential function cannot contain $\mathrm{e}^{\sqrt{3/(4x)}}$ or $\mathrm{e}^{-\sqrt{3/(4x)}}$.

2. The differential equation

$$f''(x)-x^2f'(x)+2xf(x)=0$$

has no hyperexponential solutions either. To see this, first note that the two generalized series solutions at infinity are

$$\mathrm{e}^{x^3/3}x^{-4}\Big(1+\tfrac{20}{3}x^{-3}+\tfrac{560}{9}x^{-6}+\cdots\Big)\quad\text{and}\quad x^2\Big(1-\tfrac{2}{3}x^{-3}+\tfrac{2}{9}x^{-6}+\cdots\Big).$$

Any hyperexponential solution must therefore have the kernel $\mathrm{e}^{x^3/3}$ or the kernel 1. A hyperexponential solution with kernel 1 is actually a rational function. Since the equation has no nonzero rational solutions, it has no hyperexponential solutions with kernel 1. It remains to show that there is no hyperexponential solution with kernel $\mathrm{e}^{x^3/3}$. Setting $f(x)=\mathrm{e}^{x^3/3}g(x)$ gives the differential equation

$$g''(x)+x^2g'(x)+4xg(x)=0$$

for $g(x)$. Since this equation has no nonzero rational solutions, there is also no hyperexponential solution with kernel $\mathrm{e}^{x^3/3}$.

3. Consider the differential equation

$$8(x-1)f''(x)-2(5x-7)f'(x)+(2x-15)f(x)=0.$$

Its generalized series solutions at 1 are

$$1+\tfrac{13}{4}(x-1)+\tfrac{97}{32}(x-1)^2+\cdots$$
$$\text{and }(x-1)^{1/2}\Big(1+\tfrac{3}{2}(x-1)+(x-1)^2+\cdots\Big),$$

and the generalized series solutions at infinity are

$$\mathrm{e}^{x}x^{3/2}\Big(1+\tfrac{1}{2}x^{-1}-\tfrac{5}{8}x^{-2}+\cdots\Big)$$
$$\text{and }\mathrm{e}^{x/4}x^{-2}\Big(1-\tfrac{14}{3}x^{-1}+\tfrac{89}{3}x^{-2}+\cdots\Big).$$

The main loop iterates over the kernels e^x, $e^x(x-1)^{1/2}$, $e^{x/4}$, and $e^{x/4}(x-1)^{1/2}$, of which only the second and the third pass the condition of line 6. Setting $f(x) = e^x(x-1)^{1/2}g(x)$ leads to the differential equation

$$8(x-1)g''(x) + 6(x+1)g'(x) - 6g(x) = 0$$

whose solution space in $C(x)$ is generated by $x+1$. We have thus found the hyperexponential solution $f(x) = e^x(x-1)^{1/2}(x+1)$. On the other hand, setting $f(x) = e^{x/2}g(x)$ leads to the differential equation

$$8(x-1)g''(x) - 2(3x-5)g'(x) - 12g(x) = 0$$

which has no nonzero rational solutions. We conclude that the hyperexponential solutions are precisely the constant multiples of $f(x) = e^x(x-1)^{1/2}(x+1)$.

4. Consider the differential equation

$$(x^2-4x+2)x^4f''(x) - (x^4-6x^3+12x^2-4)x^2f'(x) + (x^4-x^2+2)f(x) = 0.$$

The roots of x^2-4x+2 are apparent singularities and do not contribute to the kernel candidates. The only non-apparent singularities are 0 and infinity. At 0 we find two generalized series solutions of type $(x, \mathbb{Z})$, and at infinity there are generalized series solutions with type $(x, \mathbb{Z})$ and $(0, \mathbb{Z})$, respectively. In other words, the generalized series at 0 have the exponential part $\exp(x^{-1})$ while those at infinity have the exponential parts $\exp(x)$ and 1, respectively. This gives two kernel candidates $\exp(x+x^{-1})$ and $\exp(x^{-1})$. In this case, it turns out that both candidates give rise to hyperexponential solutions of the equation. They are $\exp(x+x^{-1})x^{-2}$ and $\exp(x^{-1})(x-2)^3x^{-1}$. Every solution of the differential equation can be viewed as a C-linear combination of these two terms, but since they are not similar, the only hyperexponential solutions are $\exp(x+x^{-1})x^{-2}$ and $\exp(x^{-1})(x-2)^3x^{-1}$ and their constant multiples.

5. For the differential equation

$$225x^4f''(x) - 30(x^3-3x^2+3x+9)x^2f'(x) + (x^6-6x^5+324x+81)f(x) = 0,$$

all generalized series solutions at zero have type $(-\frac{3}{5}x, \frac{1}{5}+\mathbb{Z})$, while those at infinity have type $(\frac{1}{30}x^2 - \frac{1}{5}x, -\frac{1}{5}+\mathbb{Z})$. The only kernel candidate is therefore $\exp(x^2/30 - x/5 - 3/(5x))x^{1/5}$. If we set the ansatz $f(x) = \exp(x^2/30 - x/5 - 3/(5x))x^{1/5}g(x)$ into the differential equation, it simplifies to the equation $225x^4g''(x) = 0$ whose solution space in $C(x)$ is generated by 1 and x. Consequently, the hyperexponential solutions of the original equation are all functions of the form $\exp(x^2/30 - x/5 - 3/(5x))x^{1/5}(c_0 + c_1x)$, where c_0, c_1 are arbitrary constants (not both zero). In this example, every element of the solution space is hyperexponential. □

The performance of Algorithm 3.74 is mainly determined by the number of iterations of the main loop. The loop iterates over all combinations of types at the various singularities. The number of these combinations can be exponential in the number of singularities, i.e., in the degree of p_r. The condition in line 6 discards a lot of combinations, but the number of combinations surviving this filter may still be very large. An implementation of the algorithm should employ further measures to reduce the number of combinations to be considered, or the amount of time spent in a single iteration. Here are some possibilities.

- If an equation has d linearly independent hyperexponential solutions which share the same type $(u_i, \alpha_i + \mathbb{Z})$ at a certain singularity ξ_i, then there must also be d linearly independent generalized series solutions with this type at ξ_i.
  If there are many hyperexponential solutions, we can use this information to avoid the inspection of some useless combinations by storing for each singularity ξ and each $(u, \alpha + \mathbb{Z})$ the dimension d of the space of all generalized series solutions at ξ whose type is $(u, \alpha+\mathbb{Z})$. Whenever we discover a hyperexponential solution with this type, we decrease the counter d. Then it suffices to only consider combinations of pairs $(u, \alpha + \mathbb{Z})$ whose associated counter is nonzero.
- A lot of combinations are discarded by line 6, and many of them for the same reason. It would be better not to even generate them. In order to generate fewer combinations, we can take one of the E_i's, say E_0, and encode it as a map which for any given class $\alpha + \mathbb{Z}$ returns the set of all u_0 such that $(u_0, \alpha + \mathbb{Z})$ belongs to E_0. Instead of going through all combinations of $E_0 \times \ldots \times E_k$, we would just go through all combinations $((u_1, \alpha_1 + \mathbb{Z}), \ldots, (u_k, \alpha_k + \mathbb{Z})) \in E_1 \times \ldots \times E_k$. Then for each of them, compute $\alpha = -(\alpha_1 + \ldots + \alpha_k)$ to get the pairs $(u_0, \alpha + \mathbb{Z})$ from E_0 and proceed with the combination $((u_0, \alpha + \mathbb{Z}), (u_1, \alpha_1 + \mathbb{Z}), \ldots, (u_k, \alpha_k + \mathbb{Z}))$.
  It is not essential that we choose infinity as the singularity whose types are selected to match a given combination of types at the other singularities. It may in fact not be the wisest choice. Instead, a reasonable choice is perhaps to take the E_i which has the largest number of distinct equivalence classes appearing in the second component of its elements.
- Once we have reached line 7 for a specific combination of types, we are left with the problem of finding rational solutions of a differential equation. As explained in the previous section, this process consists in computing a universal denominator and a degree bound for the numerator, and in solving a linear system over C. We can save time by precomputing the denominator and the degree bound, because we must have seen the relevant exponents already in the generalized series solutions. More precisely, for every type $(u_i, \alpha_i + \mathbb{Z})$ of a finite singularity $\xi_i \in C$, choose the representative α_i such that for all generalized series solutions at ξ_i with exponential part $\exp(u_i(1/(x - \xi_i)))(x - \xi_i)^\beta$ and $\beta - \alpha_i \in \mathbb{Z}$, we actually have $\beta - \alpha_i \in \mathbb{N}$, i.e., α_i is the smallest exponent that appears. With this choice of $\alpha_1, \ldots, \alpha_k$, we have that all rational solutions of the equation to be solved in line 8 are actually polynomial solutions.

If $(u, \alpha + \mathbb{Z})$ is the pair corresponding to the singularity at infinity, we again choose as α the smallest element of the equivalence class such that there is a generalized series solution of the form $\exp(u(x))(x^{-1})^{\alpha}(1 + \cdots)$. The degree of the polynomial solution is then bounded by $\alpha - (\alpha_1 + \ldots + \alpha_k)$. In particular, there are no polynomial solutions if this quantity is negative.

The denominator bounds and degree bounds can be refined during the process if we happen to discover some hyperexponential solutions. For example, if the exponents α appearing at a certain singularity are $-7, -3, 5$ and we discover a solution whose generalized series expansion has exponent -7, we can conclude that any further solutions can only have -3 or 5 as exponents, so we can use -3 instead of -7 for the denominator bound.

- We have formulated the algorithm for an algebraically closed constant field C. For realistic implementations, this is not a good assumption. If C is not algebraically closed, we are faced with the problem that the singularities $\xi_1, \ldots, \xi_k$ belong in general to certain algebraic extensions of C. Arithmetic in these extensions can be quite costly. Even worse, when we form the equation for $\tilde{y}$ in line 8, its coefficients belong to a field which may involve all of the ξ_i simultaneously, and we may have to compute a primitive element in order to properly do arithmetic with them.

  Unfortunately, there is not much we can do about this. Unlike in the previous section, where we have seen that we can always find all rational solutions without having to extend the constant field, this is no longer true for hyperexponential solutions. For example, the differential equation $x^2 f''(x) + xf'(x) - 2f(x) = 0$ has the hyperexponential solutions $x^{\sqrt{2}}$ and $x^{-\sqrt{2}}$ whose respective defining equations $xf'(x) - \sqrt{2}f(x) = 0$ and $xf'(x) + \sqrt{2}f(x) = 0$ have coefficients that belong to a larger field than the coefficients of the given equation.

  The only advice towards reducing the cost of arithmetic is to do as many computations as possible in homomorphic images. Assuming we start from $C = \mathbb{Q}$, find a prime p such that the minimal polynomials of all ξ_i's have a linear factor when viewed as polynomials over $\mathbb{Z}_p$. We can then map each ξ_i to such a root and solve the linear system for finding the polynomial solution in line 8 in the field $\mathbb{Z}_p$. If there is no solution, we proceed to the next pair, and only if a solution is found, we repeat the computation in C. Note that this can happen at most r times.

There is another way to search for hyperexponential solutions. Since the complete method is rather technical, we describe here only a simple fragment that is not guaranteed to find all hyperexponential solutions, but that can be used as an efficient preprocessor for Algorithm 3.74. The basic idea is to use a guess-and-prove approach.

To find a hyperexponential solution of a given differential equation means to find a solution of that equation which also satisfies a first order equation. If we know the initial terms of a power series expansion of a hyperexponential solution, we could use the input equation to generate many further terms of the series and then use the methods of Sect. 1.5 to guess a first order differential equation satisfied by the series.

If we find one, we can easily check whether the hyperexponential function it defines is indeed a solution of the given equation.

In order to make this approach work, we need to address two issues. First, we have to find initial values of a series solution that are likely to belong to a hyperexponential solution. Secondly, we need to know how many terms we have to supply to the guesser in order to be sure that there really is no solution if it does not find any.

Concerning the initial values, suppose that at a certain singularity ξ and a certain type $(u, \alpha + \mathbb{Z})$ the space of generalized series solutions with that type has dimension one. Then, if there is a hyperexponential solution whose generalized series expansion at ξ has the form $\exp(u(1/(x-\xi)))(x-\xi)^{\alpha+n}(1+\cdots)$ for some $n \in \mathbb{Z}$, it can only be a constant multiple of the generalized series solution at ξ of the input equation. We can therefore compute many terms of this solution and use them for guessing. If we can be sure that there is no solution, then we do not need to consider any combinations involving the pair $(u, \alpha + \mathbb{Z})$ for the singularity ξ. On the other hand, if we do find a solution, we can check which singularities it has, and what the generalized series expansions at these singularities are. We can then adjust the dimension counts accordingly in order to reduce the number of combinations.

It can happen that after the adjustment, there is a singularity ξ' and a type $(u', \alpha' + \mathbb{Z})$ for which the dimension has dropped from two to one. This means that there may be at most one further linearly independent hyperexponential solution with this type at ξ'. Suppose there is one. Then every generalized series solution at ξ' of the form $\exp(u'(1/(x-\xi')))(x-\xi')^{\alpha'+n}(1+\cdots)$ for some $n \in \mathbb{Z}$ must be the expansion of a C-linear combination of two hyperexponential functions. It must therefore satisfy a second order differential equation, which we can find by guessing. Since we already know one hyperexponential solution of this equation, it is not difficult to find the other (see Exercise 25). If this solution is indeed a solution of the original equation (which we can ensure by taking sufficiently many terms into account in the guessing part), then we can again inspect its singularities and adjust the dimension counts. If guessing with sufficiently many terms does not find a second order equation, we can conclude that there is no second hyperexponential solution with exponential part $(u', \alpha' + \mathbb{Z})$ at ξ' and we do not need to consider any combinations involving this pair for ξ'.

The process can be repeated as long as there are singularities with types for which the dimension of the space of generalized series solutions with that type exceeds the number of known linearly independent hyperexponential solutions with that type by one. After this, we can consider the remaining combinations as in Algorithm 3.74 to check whether there are further hyperexponential solutions. The procedure is summarized in the following algorithm.

Algorithm 3.77
Input and Output like for Algorithm 3.74.

Let $\xi_0 = \infty$ *and let* $\xi_1, \ldots, \xi_k \in C$ *be the roots of* p_r.
for $i = 0, \ldots, k$ *do*

Determine a finite set $E_i \subseteq C[x] \times C/\mathbb{Z}$ *such that for every generalized series solution* $\exp(u(\bar{x}))\bar{x}^{\alpha}(1+\cdots)$ *we have* $(u, \alpha+\mathbb{Z}) \in E_i$. *Here* $\bar{x}$ *refers to* $x-\xi_i$ *when* $i>0$ *and to* x^{-1} *if* $i=0$.

for every $(u, \alpha+\mathbb{Z}) \in E_i$ *do*

Let $d[i,u,\alpha+\mathbb{Z}] \in \mathbb{N}$ *be the dimension of the space of all generalized series solutions at* ξ_i *of the form* $\exp(u(\bar{x}))\bar{x}^{\alpha+n}(1+\cdots)$ *for some* $n \in \mathbb{N}$. *Let* $b[i,u,\alpha+\mathbb{Z}]=0$ *for all* i, u, α.

Set $H=\emptyset$.

while there are $i \in \{0,\dots,k\}$ *and* $(u,\alpha+\mathbb{Z}) \in E_i$ *with* $d[i,u,\alpha+\mathbb{Z}] - b[i,u,\alpha+\mathbb{Z}] = 1$ *do*

Select such i, u, α.

Compute many terms of a generalized series solution at ξ_i *with type* $(u, \alpha+\mathbb{Z})$.

Use this data to guess a differential equation of order $d[i,u,\alpha+\mathbb{Z}]$.

if there is one then

Using the $b[i,u,\alpha+\mathbb{Z}]$ *known hyperexponential solutions and Exercise 25, find a new hyperexponential solution* h *of the guessed equation, if there is one.*

if there is one then

Set $H=H\cup\{h\}$.

for $j=0,\dots,k$ *do*

Increase $b[j,\tilde{u},\tilde{\alpha}+\mathbb{Z}]$ *by one, where* $(\tilde{u},\tilde{\alpha}+\mathbb{Z})$ *is the type of the expansion of* h *at* ξ_j.

if no equation is found or the guessed equation has no new hyperexponential solution then

Set $E_i = E_i \setminus \{(u,\alpha+\mathbb{Z})\}$.

for all tuples $((u_0,\alpha_0+\mathbb{Z}),\dots,(u_k,\alpha_k+\mathbb{Z})) \in E_0\times\cdots\times E_k$ *do*

if $\sum_{i=0}^k \alpha_i \in \mathbb{Z}$ *and* $d[i,u_i,\alpha_i+\mathbb{Z}] > b[i,u_i,\alpha_i+\mathbb{Z}]$ *for all* i *then*

Set $q=\exp(u_0(x))\prod_{i=1}^k \exp(u_i(1/(x-\xi_i)))(x-\xi_i)^{\alpha_i}$.

Apply the change of variables $y=q\tilde{y}$ *to the input differential equation and find a basis* $\{b_1,\dots,b_\ell\}$ *of the space of all the rational solutions* $\tilde{y}$ *of the resulting equation.*

Set $H=H\cup\{qb_j : j=1,\dots,\ell\}$.

for $i=0,\dots,k$ *do*

Increase $b[i,\tilde{u},\tilde{\alpha}+\mathbb{Z}]$ *by* ℓ, *where* $(\tilde{u},\tilde{\alpha}+\mathbb{Z})$ *is the type of the expansion of* q *at* ξ_i.

Return H.

Example 3.78

1. Consider again the differential equation

$$8(x-1)f''(x) - 2(5x-7)f'(x) + (2x-15)f(x) = 0$$

from the previous example. Its two generalized series solutions at 1 have distinct types, so if there is a hyperexponential solution, its expansion must be one of them. The first 10 coefficients of the generalized series solution

$$(x-1)^{1/2}\bigl(1+\tfrac{3}{2}(x-1)+(x-1)^2+\tfrac{5}{12}(x-1)^3+\tfrac{1}{8}(x-1)^4+\cdots\bigr)$$

are more than enough to guess that this series satisfies the differential equation $2(x+1)(x-1)g'(x)-(2x^2+3x-3)g(x)=0$, which determines the hyperexponential function $\mathrm{e}^x(x-1)^{1/2}(x+1)$. By plugging this function into the original equation, we can easily confirm that it is a solution of that equation, so the guess was right.

In order to see if there is a second solution, we can check out the other generalized series solution at 1. It turns out that guessing does not find a first order equation for it. Alternatively, we could also try the generalized series solutions at infinity. They also have two distinct types. One of them belongs to the hyperexponential solution we have already found, and there is no point in trying to guess an equation for it (although we would find one). From the coefficients of the other solution, guessing fails to recover a first-order equation. If we offered enough terms for doing the guessing, then this means that the equation has only one hyperexponential solution.

2. Consider the second order differential equation whose solution space is generated by the hyperexponential functions $\frac{x}{\sqrt{(x+2)(x+5)}}$ and $\sqrt[3]{\frac{(x+1)(x+6)}{(x+4)^2}}$. The equation has non-apparent singularities at 0, 1, 2, 3, 4, 5, 6, and at each of them there are generalized series solutions with two distinct types. While Algorithm 3.74 has to iterate through $2^7=128$ combinations of the various types, Algorithm 3.77 will find both hyperexponential solutions by just looking at the coefficients of the two generalized series solutions at one of the singularities. □

In order to complete the discussion of the guess-and-prove approach, it remains to discuss how many series terms we need to supply to the guesser to be sure that the guesser will not overlook any solutions. Recall from Sect. 1.5 that in order to recover (or prove the absence of) an equation of order r and degree d from a series expansion, we need at least $(r+1)(d+2)$ series terms. For our present situation, this means we know the number of terms needed to bound the size of a hyperexponential solution of a given equation. Since hyperexponential solutions of differential equations correspond to right factors of differential operators, we might expect at first glance that their degree is bounded by the degree of the input equation. However, while this is true for commutative polynomials, it is in general false for differential operators. For example, the operator D^5, which has degree zero, has the right factor $(x^4+1)D-4x^3$ of degree four. The following proposition gives a bound on the size of the polynomial coefficients of first order factors of differential operators.

Proposition 3.79 *Suppose that C is algebraically closed. Let $\pi: C\to\mathbb{R}$ be a $\mathbb{Q}$-linear map with $\pi(1)=1$.*

Let $p_0, \dots, p_r \in C[x]$ with $p_r \neq 0$, let $\xi_0 = \infty$ and $\xi_1, \dots, \xi_k$ be the roots of p_r, and let $E_0, \dots, E_k$ be as computed by Algorithm 3.74.

For the types $(w, \alpha + \mathbb{Z}) \in E_i$ with $i \geq 0$, suppose the representative α of the equivalence class $\alpha + \mathbb{Z}$ is always chosen to be the smallest (i.e., left-most) element of the class which appears as an exponent in a generalized series solution at ξ_i.

Suppose that h is hyperexponential with $p_0 h + \cdots + p_r h^{(r)} = 0$, and let $q_0, q_1 \in C[x]$ be such that $\gcd(q_0, q_1) = 1$ and $q_0 h + q_1 h' = 0$. Then

$$\max(\deg(q_0), \deg(q_1)) \leq k + 2\sum_{i=0}^{k} \max_{(w,\alpha+\mathbb{Z})\in E_i} \deg(w) - \sum_{i=0}^{k} \min_{(w,\alpha+\mathbb{Z})\in E_i} \pi(\alpha).$$

□

Proof Write $h = \exp(u/v) p_0 \prod_{i=1}^{k}(x - \xi_i)_i^{\alpha}$ for some $u, v, p_0 \in C[x]$, so that

$$-\frac{q_0}{q_1} = \frac{h'}{h} = (\frac{u}{v})' + \frac{p_0'}{p_0} + \sum_{i=1}^{k} \frac{\alpha_i}{x - \xi_i}.$$

Putting the right hand side on the common denominator $v^2 p_0 \prod_{i=1}^{k}(x - \xi_i)$, we see that both numerator and denominator, i.e., both q_0 and q_1 are bounded in degree by

$$\deg(v) + \max(\deg(u), \deg(v)) + \deg(p_0) + k.$$

We have $\deg(v) \leq \sum_{i=1}^{k} \max_{(w,\alpha+\mathbb{Z})\in E_i} \deg(w)$, because the only possible roots of v are $\xi_1, \dots, \xi_k$ and their multiplicities are bounded by the largest multiplicities appearing in the exponential parts of the corresponding generalized series solutions of the equation $p_0 y + \cdots + p_r y^{(r)} = 0$. These are the $\deg(w)$.

Next, we have $\deg(u) \leq \max_{(w,\alpha+\mathbb{Z})\in E_0} \deg(w) + \deg(v)$, because the generalized series solutions of the equation $p_0 y + \cdots + p_r y^{(r)} = 0$ at infinity have exponential parts with polynomial arguments of degree at most $\max_{(w,\alpha+\mathbb{Z})\in E_0} \deg(w)$, so the expansion of u/v at infinity cannot contain larger exponents.

By combining these two estimates, we find that the degrees of q_0 and q_1 are bounded by

$$k + 2\sum_{i=0}^{k} \max_{(w,\alpha+\mathbb{Z})\in E_i} \deg(w) + \deg(p_0).$$

It remains to bound the degree of p_0. The expansion of $p_0 \prod_{i=1}^{k}(x - \xi_i)^{\alpha_i}$ at infinity is

$$x^{\deg(p_0)+\sum_{i=1}^{k}\alpha_i} + \cdots = (\frac{1}{x})^{-\deg(p_0)-\sum_{i=1}^{k}\alpha_i} + \cdots.$$

At the same time, there must be some $(w, \alpha + \mathbb{Z}) \in E_0$ and $\alpha_0 \in \alpha + \mathbb{Z}$ such that the expansion of $p_0 \prod_{i=1}^k (x - \xi_i)^{\alpha_i}$ at infinity is $(\frac{1}{x})^{\alpha_0} + \cdots$. Consequently, $\deg(p_0) = -\sum_{i=0}^k \alpha_i$, where each α_i belongs to some $\alpha + \mathbb{Z}$ with $(w, \alpha + \mathbb{Z}) \in E_i$. Since $\deg(p_0)$ is an integer, $\pi(\deg(p_0)) = \deg(p_0)$, and therefore

$$\deg(p_0) = -\sum_{i=0}^k \pi(\alpha_i) \le -\sum_{i=0}^k \min_{(w,\alpha+\mathbb{Z})\in E_i} \pi(\alpha).$$

This completes the proof. ∎

The somewhat technical appearance of the function π is needed because the exponents α of the generalized series solutions may not be real. They are elements of the constant field C on which no order is available, which prevents us from taking the minimum of exponents taken from different types of a set E_i. One way to construct a suitable function π is to construct a $\mathbb{Q}$-vector space basis B of the extension field of $\mathbb{Q}$ which contains all of the exponents α that appear in the generalized series solutions of the differential equation. It can be arranged that B contains 1, and then we can take as π the function which extracts from α the coordinate of 1 in the basis representation for B. This would work, but it has the drawback that the construction of the extension field might be very costly. A more efficient alternative is available if C is (isomorphic to) a subfield of $\mathbb{C}$. In this case, we can simply take the real part of α as $\pi(\alpha)$, and since we are only interested in a bound, a numerical evaluation of the real part will be sufficient for our purpose.

In line 9 of Algorithm 3.77 we also need a bound on the degree of higher order right factors of a differential operator, but since we are only looking for right factors which have a full basis of hyperexponential solutions, the required bound can be obtained easily by combining Proposition 3.79 with a result on closure properties.

Proposition 3.80 *Let $h_1, \ldots, h_m$ be hyperexponential and let $d \in \mathbb{N}$ be such that each h_i'/h_i is a rational function whose numerator and denominator have degrees at most d. Then there is a linear differential equation of order m with polynomial coefficients of degree at most $m^2 d$ which has $h_1, \ldots, h_m$ as solutions.* □

Proof Apply Exercise 8 of Sect. 3.3 with $r_1 = \cdots = r_m = 1$ and $d_1 = \ldots = d_m = d$. ∎

With a bound on the size of all hyperexponential solutions of a given differential equation we can formulate a third approach for finding hyperexponential solutions. We could simply make an ansatz

$$\frac{h'}{h} = -\frac{q_{0,0} + q_{0,1}x + \cdots + q_{0,d}x^d}{q_{1,0} + q_{1,1}x + \cdots + q_{1,d}x^d}$$

with unknown coefficients $q_{i,j} \in C$, plug this ansatz into the differential equation, put everything on a common denominator, equate coefficients of powers of x to zero and solve the resulting system of equations for the unknowns $q_{i,j}$. We have successfully applied similar ideas in earlier sections, but unlike there, we are now faced with a system of nonlinear equations. While it is possible to solve such systems, for example, by using Gröbner bases, we do not recommend this approach. The cost for solving the nonlinear system is so high that Algorithm 3.74 or 3.77 will be faster in almost all cases.

No matter which algorithm we use, the most common situation is that the conclusion of a time consuming computation is that the input equation has no hyperexponential solutions at all. Among all equations which do have hyperexponential solutions, almost all have only one of them (up to constant multiples of course). For equations with a hyperexponential solution, what can we say about the other solutions?

If P is the differential operator corresponding to the equation, then a hyperexponential solution corresponds to a first-order right factor of P, i.e., we have $P = P_1(v_1 D - u_1)$ for some operator P_1 and nonzero polynomials $u_1, v_1 \in C[x]$. The hyperexponential function a_1 defined by $v_1 a_1' - u_1 a_1 = 0$ is a solution of P. An additional solution of P can be constructed from a nonzero solution b_1 of P_1 by solving the inhomogeneous first order differential equation

$$b_1 = v_1 a_2' - u_1 a_2,$$

because for any solution a_2 of this equation, we have $P \cdot a_2 = P_1(v_1 D - u_1) \cdot a_2 = P_1 \cdot ((v_1 D - u_1) \cdot a_2) = P_1 \cdot b_1 = 0$. Knowing b_1, u_1, v_1, we can easily solve the equation for a_2. Setting $a_2 = ca_1$ for an unknown function c, the equation translates to

$$b_1 = v_1(c' a_1 + c a_1') - u_1 c a_1 = v_1 a_1 c',$$

so $c = \int \frac{b_1}{v_1 a_1}$, so $a_2 = a_1 \int \frac{b_1}{v_1 a_1}$.

If the solution b_1 of P_1 is hyperexponential, we can iterate the construction. We then have $P_1 = P_2(v_2 D - u_2)$ for some operator P_2 and some nonzero polynomials u_2, v_2. A solution c_1 of P_2 gives rise to a new solution $b_2 = b_1 \int \frac{c_1}{v_2 b_1}$, which in turn gives rise to a new solution

$$a_3 = a_1 \int \frac{b_2}{v_1 a_1} = a_1 \int \frac{b_1 \int \frac{c_1}{v_2 b_1}}{v_1 a_1}$$

of P. In the general case, if we have an operator P of the form $P = \cdots (v_2 D - u_2)(v_1 D - u_1)$ for some nonzero polynomials $v_1, u_1, v_2, u_2, \ldots$, let h_i $(i = 1, 2, \ldots)$ be such that $v_i h_i' - u_i h_i = 0$. Then these hyperexponential functions translate into the following solutions of P:

$$h_1, \quad h_1 \int \frac{h_2}{v_1 h_1}, \quad h_1 \int \frac{h_2 \int \frac{h_3}{v_2 h_2}}{v_1 h_1}, \quad h_1 \int \frac{h_2 \int \frac{h_3 \int \frac{h_4}{v_3 h_3}}{v_2 h_2}}{v_1 h_1}, \quad \ldots$$

These solutions are called *d'Alembertian* solutions of P. It is not difficult to show (Exercise 28) that these solutions are linearly independent over C.

Example 3.81 Consider once more the equation

$$8(x-1)f''(x) - 2(5x-7)f'(x) + (2x-15)f(x) = 0$$

from before. We already know that it has the hyperexponential solution $h_1 = \mathrm{e}^x(x-1)^{1/2}(x+1)$ and no others. This solution indicates that the differential operator $P = 8(x-1)D^2 - 2(5x-7)D + (2x-15)$ has the right factor $2(x-1)(x+1)D - (2x^2+3x-3)$. In fact, we have the factorization

$$\begin{aligned} &8(x-1)D^2 - 2(5x-7)D + (2x-15) \\ &\quad = \frac{1}{1+x}(4D-1)\big(2(x-1)(x+1)D - (2x^2+3x-3)\big). \end{aligned}$$

The left factor $4D-1$ has the solution $h_2 = \mathrm{e}^{-x/4}$, which translates into the second solution

$$\begin{aligned} &\mathrm{e}^x(x-1)^{1/2}(x+1) \int \frac{\mathrm{e}^{-x/4}}{\mathrm{e}^x(x-1)^{1/2}(x+1)} \\ &\quad = \mathrm{e}^x(x-1)^{1/2}(x+1) \int \frac{\mathrm{e}^{-5x/4}}{(x-1)^{1/2}(x+1)}. \end{aligned}$$

□

Exercises

1. Show that the product of two hyperexponential functions is hyperexponential.

2. Show that the composition of a hyperexponential function with a rational function is hyperexponential.

3. Prove or disprove: The composition of a hyperexponential function with a radical (i.e., a fractional power of a rational function, such as $(x-1)^{1/3}$) is hyperexponential.

4. Show that if h is a hyperexponential function, then so is h^q for any $q \in \mathbb{Q}$.

5****.** Let $g \in C(x)$, let $h_1, \dots, h_m \in C[x] \setminus C$ be squarefree and pairwise coprime, and let $\alpha_1, \dots, \alpha_m \in C \setminus \{0\}$. Let $f(x) = \exp(g(x)) \prod_{i=1}^m h_i(x)^{\alpha_i}$. Prove or disprove:

a. $f(x)$ is exponential if and only if $m = 0$.

b. $f(x)$ is a kernel if and only if $\alpha_1, \dots, \alpha_m \notin \mathbb{Z}$.

6***.** Let K be a differential field and let E be a differential extension with $\mathrm{Const}(K) = \mathrm{Const}(E)$. Let $y_1, y_2 \in E$ be hyperexponential over K. Show that $y_1 + y_2$ is hyperexponential if and only if $y_1/y_2 \in K$.

7***.** Let K be a differential field and let E be a differential extension with $\mathrm{Const}(K) = \mathrm{Const}(E)$. Suppose that $y \in E$ is algebraic and hyperexponential over K. Show that there exists $d \in \mathbb{N}$ such that $y^d \in K$.

8****.** Let K be a differential field, let $q \in K$, and consider a transcendental extension $E = K(h)$ with $D(h) = qh$. Show that $\mathrm{Const}(E) = \mathrm{Const}(K)$ if and only if the differential equation $D(y) = qy$ has no nonzero solutions that are algebraic over K.

Hint: Use the fact shown in the previous exercise.

9. Suppose that h_1, h_2 are two hyperexponential functions which are not similar to each other, and suppose that their sum $h_1 + h_2$ is a solution of a differential equation. Show that h_1 and h_2 must also be solutions of this equation.

10. Show that we cannot drop the assumption that h_1, h_2 are not similar in the previous exercise.

11. Prove or disprove: Every hyperexponential function is either exponential or algebraic.

12. Prove or disprove: A rational function is exponential if and only if it is constant.

13. Find the hyperexponential solutions of the following inhomogeneous equations:

a. $(x+1)f''(x) - 6f'(x) + f(x) = \frac{x(x^2-17)}{(x+1)^2}\mathrm{e}^x$;

b. $(x+1)f''(x) + (x^2+1)f'(x) - (x^2+1)f(x) = (x+1)\mathrm{e}^x$.

14. Find hyperexponential closed forms for the following integrals, if there are any: **a.** $\int \frac{(x-1)^2(220x^2-270x+93)\mathrm{e}^{x-x^2}}{(x+1)^{3/2}}$; **b.** $\int \frac{(x-1)^2(220x^2+270x+93)\mathrm{e}^{x-x^2}}{(x+1)^{3/2}}$.

15. Show that two hyperexponential functions are similar if and only if they have the same set of kernels.

16. Determine all ways to write $\exp((x+1)^2/x)(x+2)^{1/2}(x+3)^{-1/5}(x+4)$ as a product of a shell and a kernel.

17. Find a solution in $C(x)$ of the following nonlinear differential equation:

$$q'(x) = \frac{2}{3(x+1)^2} - \frac{4x+1}{3(x+1)^2}q(x) - q(x)^2.$$

Hint: Translate the problem to the search for a hyperexponential solution of a linear differential equation.

18. The hyperexponential functions $h_1 = \exp(2x)x^3$, $h_2 = \exp(-x)x^{2/3}$, $h_3 = \exp(3x)x^{-1/3}$ are transcendental, but not algebraically independent over $C(x)$. Find a nonzero polynomial $p \in C(x)[y_1, y_2, y_3]$ such that $p(h_1, h_2, h_3) = 0$.

19. Find the hyperexponential solutions of the following equations:

a. $2(x+1)f''(x) + 2(x+3)f'(x) - (x-1)f(x) = 0$;
b. $(x-1)f''(x) - (2x-1)^2 f'(x) + 4(2x-1)f(x) = 0$;
c. $(x-1)f''(x) - (2x-1)^2 f'(x) - 4(2x-1)f(x) = 0$;
d. $x^4 f''(x) - (8x^5 - 6x^4 + x^3 - 2x^2)f'(x) + (16x^6 - 24x^5 + 9x^4 - 11x^3 + 3x^2 - 3x + 1)f(x) = 0$;
e. $(3x+4)(3x+1)^2 f''(x) + (9x^2 - 12x - 23)(3x+1)f'(x) - 6(9x^2 - 3x - 11)f(x) = 0$.

20. Find all constants α for which the equation

$$(\alpha x + 1)(2\alpha x + 1)f(x) + (2\alpha x^2 + 5\alpha x + 4\alpha - x)f'(x) + (x+1)f''(x) = 0$$

has a hyperexponential solution.

21. Construct a differential equation with the hyperexponential solutions $\mathrm{e}^x(x+1)^{1/9}$ and $\mathrm{e}^{x/9}(x+1)^{-1}$.

22*. Are the hyperexponential functions returned by Algorithm 3.74 always C-linearly independent?

23. Prove or disprove: If a differential equation has a d'Alembertian solution of the form $h_1 \int \frac{h_2}{v_1 h_1}$, where h_1, h_2 are some hyperexponential functions and h_1 satisfies $u_1 h_1 - v_1 h_1' = 0$ for some polynomial u_1, then h_1 must also be a solution of that equation.

24. Prove or disprove: An equation of order two has either no hyperexponential solution or two linearly independent hyperexponential solutions.

25. Let L be a differential operator of order $r-1$. Let $u, v \in C[x]$, $v \neq 0$, and $P = (u - vD)L$. Let h be a hyperexponential function with $uh - vh' = 0$. Show that any hyperexponential solution f of P which is not already a solution of L is a solution of the inhomogeneous equation $Lf = h$.

26. While a polynomial can have multiple roots, a differential equation cannot have multiple solutions. However, a differential equation can have multiple factors. What are the two solutions of the operator $(u - vD)^2$?

27. Suppose that C is algebraically closed. Show that every differential equation $c_0 y + \cdots + c_r y^{(r)} = 0$ with $c_0, \ldots, c_r \in C$, $c_r \neq 0$ has r linearly independent hyperexponential solutions.

28. Let $P = \cdots (v_3 D - u_3)(v_2 D - u_2)(v_1 D - u_1)$ be a differential operator with coefficients in $C[x]$. For each $i = 1, 2, 3, \ldots$, let h_i be a hyperexponential function with $(v_i D - u_i) \cdot h_i = 0$. Show that the d'Alembertian solutions

$$a_1 = h_1, \quad a_2 = h_1 \int \frac{h_2}{v_1 h_1}, \quad a_3 = h_1 \int \frac{h_2 \int \frac{h_3}{v_2 h_2}}{v_1 h_1}, \ldots$$

of P are linearly independent over C.

Hint: We have $(v_{i-1} D - u_{i-1}) \cdots (v_1 D - u_1) \cdot a_i = h_i$ for $i = 2, 3, \ldots$

References

The basic idea of Algorithm 3.74 for finding hyperexponential solutions was known in the nineteenth century. Beke's paper [52] contains a sketch of the algorithm. The additional idea used in Algorithm 3.77 as a preprocessor of the classical algorithm is due to van Hoeij, who pushed it a bit further than explained here and obtained a complete algorithm for finding hyperexponential solutions [443] that does not need to fall back to Algorithm 3.74. However, also van Hoeij's algorithm includes a combination step that causes exponential runtime. Another algorithm, introduced by Johansson, Kauers, and Mezzarobba [254], solves the combination problem in polynomial time using effective analytic continuation. So far, no implementation of this algorithm is available.

Cluzeau and van Hoeij [160] discuss the use of homomorphic images in the context of finding hyperexponential solutions.

In Sect. 2.6 we have seen two algorithms for finding hypergeometric solutions of recurrences. Algorithm 2.82 can be viewed as a recurrence analog of Algorithm 3.74. An algorithm for finding hyperexponential solutions which can be viewed as a differential analog of Algorithm 2.75 is explained in some lecture notes of Li [311].

Abramov and Petkovšek [15] discuss d'Alembertian solutions of linear differential and difference equations. Algorithms for finding solutions of even more advanced type are known but beyond the scope of this book. There is an algorithm by Singer [406] which finds all algebraic solutions of a given linear differential equation with polynomial coefficients. An algorithm due to Kovacic [295] finds all liouvillean solutions of a given linear differential equation of order 2 with polynomial coefficients. To be liouvillean means to belong to a differential field of the form $C(x)(t_1, \ldots, t_n)$, where for each $i \in \{1, \ldots, n\}$ we either have $t_i'/t_i \in C(x)(t_1, \ldots, t_{i-1})$ or $t_i' \in C(x)(t_1, \ldots, t_{i-1})$ or t_i is algebraic over $C(x)(t_1, \ldots, t_{i-1})$. Kovacic's algorithm has been generalized by Singer [408] to differential equations of arbitrary order whose coefficients may be liouvillean functions. While Kovacic's algorithm works in practice and is implemented in many computer algebra systems, Singer's algorithms for finding algebraic or liouvillean solutions are so far only of theoretical interest. As Bronstein already remarked in 1992 [110], the design of fast general solvers for higher order equations depends in an essential way on having a fast solver for hyperexponential solutions.

There are also some approaches to finding certain types of non-liouvillean solutions of a given differential equation, for example, solutions that can be expressed in terms of Bessel functions [169, 449] or more generally solutions that can be expressed in terms of a hypergeometric ${}_2F_1$ [245, 301, 461].

Chapter 4
Operators

4.1 Ore Algebras and Ore Actions

Chapters 2 and 3 have been written to highlight the parallels between differential and recurrence equations. We have seen that most things (definitions, theorems, algorithms, etc.) laid out in one chapter have a natural counterpart in the other chapter. Our goal is now to develop a more general theory that includes both differential equations and recurrence equations as special cases by adopting the viewpoint of operators. In fact, we have already used differential operators and recurrence operators without formally introducing them: they were viewed as polynomials $p_0 + p_1X + \cdots + p_rX^r$, where X played the role of derivation or shift, multiplied by coefficients p_i. In order to get the desired property that $(LM) \cdot f = L \cdot (M \cdot f)$, i.e., that the product of two operators acts on a function in the same way as the two factors act in succession, we were forced to give up commutativity of the multiplication. For example, if we write a function f very explicitly in the form $(t \mapsto f(t))$, then we have $x \cdot (D \cdot f) = (t \mapsto tf'(t))$ and $D \cdot (x \cdot f) = (t \mapsto tf'(t) + f(t))$, so the operators xD and Dx cannot be equal. Instead, we need that $Dx = xD+1$. Similarly, we have $x \cdot (S \cdot f) = (t \mapsto tf(t+1))$ and $S \cdot (x \cdot f) = (t \mapsto (t+1)f(t+1))$, so the operators xS and Sx cannot be equal either. Instead, we need to have $Sx = (x+1)S$. These so-called *commutation rules* motivate the following definition.

Definition 4.1 Let R be a ring.

1. If $\sigma\colon R \to R$ is a ring endomorphism and $\delta\colon R \to R$ is such that $\delta(a+b) = \delta(a)+\delta(b)$ and $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$ for all $a, b \in R$, then δ is called a σ-*derivation*. The subset $\mathrm{Const}(R) = \mathrm{Const}_{\sigma,\delta}(R) = \{c \in R : \sigma(c) = c \wedge \delta(c) = 0\}$ of R is called the *constant ring* of R (with respect to σ and δ).
2. Suppose that a ring structure is defined on the set $R[X]$ of univariate polynomials in X with coefficients in R, and suppose that its addition agrees with the usual addition and its multiplication is such that $X^iX^j = X^{i+j}$ ($i, j \in \mathbb{N}$) and there

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1_4

is an endomorphism $\sigma\colon R \to R$ and a σ-derivation $\delta\colon R \to R$ such that $Xa = \sigma(a)X + \delta(a)$ for all $a \in R$. Suppose further that the multiplication in $R[X]$ extends the multiplication of R in the sense that $R[X]$ is a left-R-module. Then $R[X]$ is called an *Ore algebra* over R. □

Since the multiplication in $R[X]$ need not be commutative, we should insist on the convention that polynomials have the form $p_0 + p_1X + \cdots + p_rX^r$, i.e., the coefficients p_i are placed on the left side of the terms X^i. Note that whenever a polynomial is given in some other form (e.g., with all coefficients on the left, or even with mixed terms such as pX^iqX^jr), a repeated application of the commutation rules always allow us to bring them into the standard form where all coefficients are on the left (see also Theorem 4.3 below). This form is unique because the powers of X are understood to be linearly independent over R.

Example 4.2

1. The ring $C[x][D]$ of differential operators is an Ore algebra. This ring is known as the first Weyl algebra. We have $\sigma = \mathrm{id}$ and $\delta = \frac{d}{dx}$. Also, the ring $C(x)[D]$ of differential operators is an Ore algebra for which we have $\sigma = \mathrm{id}$ and $\delta = \frac{d}{dx}$. Even more generally, if R is any differential ring, then $R[D]$ is an Ore algebra with $\sigma = \mathrm{id}$ and δ being the derivation of R.
   In $C[x][D]$ we have, for example,
   $$\begin{aligned}(aD+b)(cD+d) &= (aD+b)cD + (aD+b)d\\ &= a(cD+c')D + bcD + a(dD+d') + bd\\ &= acD^2 + (ac' + bc + ad)D + (ad' + bd),\end{aligned}$$
   where c', d' refer to the derivatives of c, d.
2. The Euler derivation is defined as $\theta := x\frac{d}{dx}$. The ring $C[x][\theta]$ of Euler-differential operators is an Ore algebra with $\sigma = \mathrm{id}$ and $\delta = x\frac{d}{dx}$.
3. The ring $C[x][S]$ of recurrence operators is an Ore algebra. In this case, σ is the function that maps $p(x) \in C[x]$ to $p(x+1)$, and δ is identically zero. Again, we may take $C(x)$ instead of $C[x]$, and, more generally, if R is any difference ring, then $R[S]$ is an Ore algebra with σ being the endomorphism of R and δ being identically zero.
   For example, in $C[x][S]$ we have
   $$\begin{aligned}(aS+b)(cS+d) &= aScS + aSd + bcS + bd\\ &= a\sigma(c)S^2 + (a\sigma(d) + bc)S + bd.\end{aligned}$$
4. Let $q \in C$ be fixed and define the q-shift S_q by $(S_qf)(x) = f(qx)$. The set $C[x][S_q]$ of all q-shift-recurrence operators $p_0 + p_1S_q + \cdots + p_rS_q^r$ forms an Ore algebra with $\sigma\colon C[x] \to C[x]$ as the function that maps $p(x)$ to $p(qx)$ and δ being identically zero. Since $C[x]$ together with σ is a difference ring,

this example is just another special case of an Ore algebra $R[S]$ with R being a difference ring.

5. Another special case is the Ore algebra $C[x][M_q]$ of Mahler operators. Here, for a fixed $q \in \mathbb{N}$ the operator M_q is defined through $(M_q f)(x) = f(x^q)$. The corresponding ring of linear operators $p_0 + p_1 M_q + \cdots + p_r M_q^r$ forms an Ore algebra with $\sigma\colon C[x] \to C[x]$ being the function that maps $p(x)$ to $p(x^q)$ and with δ being the zero function.
6. As an alternative to recurrence equations, we can consider difference equations, which are expressed in terms of the forward difference operator Δ defined via $(\Delta f)(x) = f(x+1) - f(x)$. The ring $C[x][\Delta]$ of all operators of the form $p_0 + p_1\Delta + \cdots + p_r\Delta^r$ is an Ore algebra with the shift as σ (as in the previous case) and the function that maps $p(x) \in C[x]$ to $p(x+1) - p(x)$ as δ. It can be checked (Exercise 1) that this δ is indeed a σ-derivation.
7. Let $C = \mathbb{Q}(\alpha)$ be an algebraic number field and let σ be an element of the Galois group of C over $\mathbb{Q}$. Then there is an Ore algebra $C[X]$ with the commutation rule $Xa = \sigma(a)X$ for all $a \in C$.
   More specifically, take $C = \mathbb{C}$ and let σ be the conjugation map, i.e., $\sigma(a+b\mathrm{i}) = \overline{a+b\mathrm{i}} = a - b\mathrm{i}$ for any $a, b \in \mathbb{R}$. Then there is an Ore algebra $\mathbb{C}[X]$ with the commutation rule $Xa = \bar{a}X$ for all $a \in \mathbb{C}$.
8. Let C be a field of characteristic $p > 0$ and let $\sigma\colon C \to C$ be the Frobenius endomorphism defined by $\sigma(a) = a^p$ for all $a \in C$. Then there is an Ore algebra $C[X]$ with the commutation rule $Xa = \sigma(a)X$ for all $a \in C$.
9. It is not required that the ground ring R is commutative or free of zero divisors. For example, let $R = C^{2\times 2}$, $A = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 4 \end{smallmatrix}\right)$, and define $\delta\colon R \to R$ by $\delta(M) = MA - AM$. Then δ is a derivation on R and there is an Ore algebra $R[X]$ whose commutation rule is $Xa = aX + \delta(a)$. □

Are all of the Ore algebras mentioned in the example above really well-defined? On the one hand, it is easy to see that a commutation rule $Xa = \sigma(a)X + \delta(a)$ can only work if σ is an endomorphism and δ is a σ-derivation. To see this, just observe that

$$Xab = (Xa)b = (\sigma(a)X + \delta(a))b = \sigma(a)\sigma(b)X + (\delta(a)b + \sigma(a)\delta(b)),$$
$$Xab = X(ab) = \sigma(ab)X + \delta(ab),$$

so $\sigma(ab) = \sigma(a)\sigma(b)$ and $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$ for all $a, b \in R$. So the restrictions on σ and δ are necessary. On the other hand, it could be questioned whether the conditions imposed on σ and δ are also sufficient, i.e., whether every choice of σ and δ indeed gives rise to an Ore algebra. The following theorem asserts that this is the case.

Theorem 4.3 *Let R be a ring, $\sigma\colon R \to R$ an endomorphism, and $\delta\colon R \to R$ a σ-derivation. Then there exists exactly one Ore algebra $R[X]$ with $Xa = \sigma(a)X + \delta(a)$ for all $a \in R$.* □

Proof We already know that $R[X]$ together with the usual addition forms an abelian group. We have to show that there is a unique way to define a multiplication on $R[X]$ that is compatible with this addition and satisfies the required commutation rule. To be compatible means that it should be associative and that it should satisfy the two distributive laws.

Distributivity enforces

$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{m}(a_i X^i)(b_j X^j)$$

for any choice of $a_0, \dots, a_n, b_0, \dots, b_m \in R$. For each of the terms $(a_i X^i)(b_j X^j)$, associativity enforces $(a_i X^i)(b_j X^j) = a_i(X^i b_j)X^j$. The desired commutation rule enforces $X^i b_j = X^{i-1}(Xb_j) = X^{i-1}\sigma(b_j)X + X^{i-1}\delta(b_j)$, and, by induction on i, that there is at most one choice of $c_0, \dots, c_i \in R$ such that $X^i b_j = c_0 + c_1 X + \dots + c_i X^i$. Since $X^i X^j = X^{i+j}$ for all $i, j \in \mathbb{N}$ and the multiplication of coefficients must agree with the multiplication of the ground ring, it follows that we must have $(a_i X^i)(b_j X^j) = (a_i c_0)X^j + (a_i c_1)X^{1+j} + \dots + (a_i c_i)X^{i+j}$. It is therefore shown that there is *at most* one Ore algebra for a given pair (σ, δ).

For the existence, first define inductively $\gamma(u, k, n)$ for every $u \in R$, every $n \in \mathbb{N}$, and every $k \in \mathbb{Z}$ by $\gamma(u, 0, 0) = u$, $\gamma(u, k, 0) = 0$ for $k \neq 0$, $\gamma(u, k, n) = 0$ for $k < 0$, and $\gamma(u, k, n + 1) = \sigma(\gamma(u, k - 1, n)) + \delta(\gamma(u, k, n))$. Note that this definition implies $\gamma(u, k, n) = 0$ for $k > n$. We define $X^n u := \sum_k \gamma(u, k, n)X^k$ for every $n \in \mathbb{N}$ and set

$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) := \sum_{i=0}^{n}\sum_{j=0}^{m} a_i(X^i b_j)X^j.$$

The distributive laws and the commutation rule $Xu = \sigma(u)X + \delta(u)$ $(u \in R)$ are then satisfied by construction, and it remains to check associativity. Because of distributivity, it suffices to check that $((aX^i)(bX^j))(cX^k) = (aX^i)((bX^j)(cX^k))$ for all $a, b, c \in R$ and $i, j, k \in \mathbb{N}$. In fact, it even suffices to check $(XbX^k)c = X(bX^k c)$ for all $b, c \in R$ and all $k \in \mathbb{N}$, because the case $i > 1$ can be treated by induction, and multiplying with an element of R from the left or with a power of X from the right is harmless. For all $b, c \in R$ and $k \in \mathbb{N}$ we have

$$\begin{aligned}
(XbX^k)c &= \sigma(b)X^{k+1}c + \delta(b)X^k c \\
&= \sum_j \big(\sigma(b)\gamma(c, j, k+1) + \delta(b)\gamma(c, j, k)\big)X^j \\
&= \sum_j \big(\sigma(b)\sigma(\gamma(c, j-1, k)) + \sigma(b)\delta(\gamma(c, j, k)) + \delta(b)\gamma(c, j, k)\big)X^j,
\end{aligned}$$

$$\begin{aligned}X(bX^k c) &= \sum_j Xb\gamma(c,j,k)X^j\\ &= \sum_j \sigma(b\gamma(c,j,k))X^{j+1} + \delta(b\gamma(c,j,k))X^j\\ &= \sum_j \big(\sigma(b)\sigma(\gamma(c,j-1,k)) + \delta(b)\gamma(c,j,k) + \sigma(b)\delta(\gamma(c,j,k))\big)X^j,\end{aligned}$$

and since both quantities agree, the proof is complete. ■

Implicit in the above proof is the following multiplication algorithm for elements of Ore algebras.

Algorithm 4.4
Input: *Two elements* $P = p_0 + p_1X + \cdots + p_rX^r$ *and* Q *of an Ore algebra* $R[X]$
Output: *The product* $PQ \in R[X]$

Set $R = 0$.
for $i = 0, \ldots, r$ *do*
  $R = R + p_iQ$ *(here* p_i *is multiplied to the left of each coefficient of* Q*).*
  $Q = \sigma(Q)X + \delta(Q)$ *(here the understanding is that* σ, δ *are applied to the coefficients of* Q*).*
Return R.

Some authors use notations like $R\langle X\rangle$ to emphasize the non-commutativity of an Ore algebra. Others write $R[X;\sigma,\delta]$ in order to include the two functions governing the commutation rules into the notation. We will stick to the common notation $R[X]$ for univariate polynomials, but instead of X we will often use the symbol ∂ (not to be confused with δ) for denoting the indeterminate. With this notation, the elements of $R[\partial]$ look more like operators. Note however that the formal construction does not require that the elements of $R[\partial]$ are operators, we just use them primarily for that purpose.

The commutation rule strongly restricts the non-commutativity of an Ore algebra, to the effect that Ore algebras are more closely related to commutative polynomial rings than to more general non-commutative rings.

Definition 4.5 Let $R[\partial]$ be an Ore algebra.

1. The *order* of a nonzero element $L \in R[\partial]$ is defined as the largest $r \in \mathbb{N}$ such that the coefficient $[\partial^r]L$ of ∂^r in L is nonzero. It is denoted by $\operatorname{ord}(L)$. We also define $\operatorname{ord}(0) = -\infty$.
2. For an element $L \in R[\partial] \setminus \{0\}$, the coefficient $\operatorname{lc}(L) := [\partial^{\operatorname{ord}(L)}]L$ is called the *leading coefficient,* and $\operatorname{lt}(L) = \partial^{\operatorname{ord}(L)}$ is called the *leading term.* $L \in R[\partial]$ is called *monic* if $\operatorname{lc}(L) = 1$.
3. A nonzero element L of a left ideal I of $R[\partial]$ is called *minimal* if $\operatorname{ord}(M) \geq \operatorname{ord}(L)$ for all nonzero elements M of I. □

Proposition 4.6 *Let* $R[\partial]$ *be an Ore algebra.*

1. *We have* $\operatorname{ord}(ML) = \operatorname{ord}(M) + \operatorname{ord}(L)$ *for all* $M, L \in R[\partial]$ *if and only if* σ *is injective and* R *is an integral domain.*
2. *Suppose that* σ *is injective and* R *is an integral domain. Then every left ideal* $I \neq \{0\}$ *of* $R[\partial]$ *has a unique monic minimal element if and only if* R *is in fact a field.* □

Proof

1. "⇒": For $p \in \ker\sigma \setminus \{0\}$, we have $\partial p = \sigma(p)\partial + \delta(p) = \delta(p)$, so $\operatorname{ord}(\partial p) < \operatorname{ord}(\partial) + \operatorname{ord}(p)$ in contradiction to the assumption. Also, for any $u, v \in R \setminus \{0\}$ with $uv = 0$, we have $\operatorname{ord}(uv) < \operatorname{ord}(u) + \operatorname{ord}(v)$ in contradiction to the assumption.
   "⇐": For any $L = \ell_n\partial^n + \cdots$, $M = m_k\partial^k + \cdots$ in $R[\partial]$ we have $LM = \ell_n\sigma^n(m_k)\partial^{n+k} + \cdots$, and the assumptions guarantee that $\ell_n\sigma^n(m_k)$ is nonzero if ℓ_n and m_k are nonzero.
2. "⇒": If R is not a field, then it has some non-invertible element $p \in R$. The left ideal $\langle p\rangle$ generated by p in $R[\partial]$ contains an element of order 0 (namely p), but no monic element of order 0 (i.e., it does not contain 1). To see this, observe that every element of $\langle p\rangle$ has the form $Lp = (\ell_n\partial^n + \cdots + \ell_0)p = \ell_n\sigma^n(p)\partial^n + \cdots$, and by the assumptions on R and σ, the coefficient $\ell_n\sigma^n(p)$ is not zero when ℓ_n is not zero. So in order for Lp to have order 0, we must have $n = 0$, but then $Lp = \ell_0 p$ cannot be 1 because p was assumed not to be invertible in R.
   "⇐": If L is any element of I for which $\operatorname{ord}(L)$ is minimal, then $\operatorname{lc}(L)^{-1}L$ is a monic minimal element of I, so monic minimal elements always exist. If L_1, L_2 are two monic minimal elements of I, then $\operatorname{ord}(L_1) = \operatorname{ord}(L_2)$ and $\operatorname{lc}(L_1) = \operatorname{lc}(L_2) = 1$ implies that $\operatorname{ord}(L_1 - L_2) < \operatorname{ord}(L_1) = \operatorname{ord}(L_2)$, which by minimality of L_1, L_2 implies that $L_1 - L_2 = 0$, i.e., $L_1 = L_2$. ■

From a formal perspective, the elements of an Ore algebra $R[\partial]$ become operators as soon as we have a left-$R[\partial]$-module F on which they can act. In view of the applications we have in mind, we call such modules *function spaces*. Recall that to be a left-$R[\partial]$-module means that there is an addition $+\colon F \times F \to F$ which turns F into an abelian group and a multiplication $\cdot\colon R[\partial] \times F \to F$ which satisfies the rules

$$\begin{aligned} 1 \cdot f &= f, \\ (L + M) \cdot f &= (L \cdot f) + (M \cdot f), \\ L \cdot (f + g) &= (L \cdot f) + (L \cdot g), \\ (LM) \cdot f &= L \cdot (M \cdot f), \end{aligned}$$

for all $L, M \in R[\partial]$ and all $f, g \in F$. For example, the ring $C[[x]]$ of formal power series is a left-$C[x][D]$-module if we define multiplication via

$$(p_0 + p_1 D + \cdots + p_r D^r) \cdot f = p_0 f + p_1 f' + \cdots + p_r f^{(r)}.$$

Definition 4.7 Let $R[\partial]$ be an Ore algebra and F be a left-$R[\partial]$-module.

1. For $f \in F$, we call $\operatorname{ann}(f) = \{L \in R[\partial] : L \cdot f = 0\}$ the *annihilator* of f (in $R[\partial]$).
2. $f \in F$ is *D-finite* (with respect to the action of $R[\partial]$ on F) if $\operatorname{ann}(f) \neq \{0\}$.
3. For $L \in R[\partial]$, we call $V(L) = \{f \in F : L \cdot f = 0\}$ the *solution space* of L (in F). □

Example 4.8

1. Taking $C[x][D]$ as $R[\partial]$ and $C[[x]]$ as F, we have

$$D - 1 \in \operatorname{ann}(\exp(x)) \quad \text{and} \quad \exp(x) \in V(D-1),$$

   because $(D-1) \cdot \exp(x) = 0$. Note that we also have $5\exp(x) \in V(D-1)$ and $xD - x \in \operatorname{ann}(\exp(x))$.
2. Taking $C[x][S]$ as $R[\partial]$ and $C^{\mathbb{N}}$ as F, we have

$$S - 2 \in \operatorname{ann}((2^n)_{n=0}^{\infty}) \quad \text{and} \quad (2^n)_{n=0}^{\infty} \in V(S-2),$$

   because $(S-2) \cdot (2^n)_{n=0}^{\infty} = (0)_{n=0}^{\infty}$. We also have $(c\,2^n)_{n=0}^{\infty} \in V(S-2)$ for any $c \in C$ and $xS - 2x \in \operatorname{ann}((2^n)_{n=0}^{\infty})$, but, for example, $S - x \notin \operatorname{ann}((2^n)_{n=0}^{\infty})$, because $(S-x) \cdot (2^n)_{n=0}^{\infty} = (2^{n+1} - n2^n)_{n=0}^{\infty} = ((2-n)2^n)_{n=0}^{\infty} \neq (0)_{n=0}^{\infty}$.
3. The definition of D-finiteness is compatible with the definitions we gave earlier for the shift and differential case, and it covers other cases as well. For example, if we let the Ore algebra $C(x)[M_2]$ of Mahler operators act on $C((x))$, we find that $(xM_2 - 1) \cdot \frac{1}{x} = x\frac{1}{x^2} - \frac{1}{x} = 0$, so $\frac{1}{x}$ is D-finite. Other examples such as $\exp(x)$ are not D-finite in this setting (Exercise 13), and $\sum_{n=0}^{\infty} x^{2^n}$ is D-finite with respect to $C(x)[M_2]$ (an annihilating operator is $M_2^2 - 2M_2 + 1$) but it is not D-finite with respect to $C(x)[D]$ (Exercise 3 in Sect. 3.1).
4. If $R[\partial]$ is an Ore algebra, then $R[\partial]$ is naturally a left-module over itself. Also R can be viewed as a left-$R[\partial]$-module. If we set $\partial \cdot 1 := u$ for some element $u \in R$ of our choice, then $\partial \cdot r = (\partial r) \cdot 1 = (\sigma(r)\partial + \delta(r)) = \sigma(r)u + \delta(r)$ fixes the action. As a concrete example, think of the natural action of $C[x][D]$ on $C[x]$. Here we have $D \cdot 1 = 0$, which implies that $D \cdot r = \delta(r)$ for all $r \in C[x]$. On the other hand, for the natural action of $C[x][S]$ on $C[x]$, we have $S \cdot 1 = 1$, which together with $\delta = 0$ implies $S \cdot r = \sigma(r)$ for all $r \in C[x]$. □

Theorem 4.9 *Let $R[\partial]$ be an Ore algebra and F be a left-$R[\partial]$-module. Let $f \in F$ and $L \in R[\partial]$.*

1. $\operatorname{ann}(f)$ *is a left ideal of* $R[\partial]$.
2. $V(L)$ *is a* $\operatorname{Const}(R)$*-submodule of* F. □

Proof Both parts of the proof depend on the observation that $L \cdot 0 = 0$ for all $L \in R[\partial]$, which follows from the calculation $L \cdot 0 = L \cdot (0+0) = (L \cdot 0) + (L \cdot 0)$.

1. Clearly $\operatorname{ann}(f)$ is not empty because $0 \cdot f = 0$, so $0 \in \operatorname{ann}(f)$. Let $L_1, L_2 \in \operatorname{ann}(f)$ and $M_1, M_2 \in R[\partial]$. Then $(M_1L_1+M_2L_2)\cdot f = ((M_1L_1)\cdot f)+((M_2L_2)\cdot f) = (M_1 \cdot (L_1 \cdot f)) + (M_2 \cdot (L_2 \cdot f)) = (M_1 \cdot 0) + (M_2 \cdot 0) = 0 + 0 = 0$, so $M_1L_1 + M_2L_2 \in \operatorname{ann}(f)$.
2. Clearly $V(L)$ is not empty because $L \cdot 0 = 0$, so $0 \in V(L)$. Let $f, g \in V(L)$ and $\alpha, \beta \in \operatorname{Const}(R)$. Write $L = p_0 + p_1\partial + \cdots + p_r\partial^r$ with $p_0, \ldots, p_r \in R$, so that $L \cdot f = L \cdot g = 0$. Then $L \cdot ((\alpha \cdot f) + (\beta \cdot g)) = ((L\alpha) \cdot f) + ((L\beta) \cdot g) = (\alpha \cdot (L \cdot f)) + (\beta \cdot (L \cdot g)) = (\alpha \cdot 0) + (\beta \cdot 0) = 0+0 = 0$, so $(\alpha \cdot f) + (\beta \cdot g) \in V(L)$. ■

The second part of the theorem looks more familiar if we apply it to the typical situation where $R = C(x)$ or $R = C[x]$ and an Ore algebra $R[\partial]$ where ∂ commutes with all elements of C but not with x. If $\partial = D$ or $\partial = S$, we have $\operatorname{Const}(R) = C$ and the statement reduces to the fact that $V(L)$ is a C-vector space. In general, the solution space $V(L)$ is not closed under multiplication by x or under application of ∂.

For any element $f \in F$, we can consider the left-$R[\partial]$-module generated by f in F. This is the set of all elements of F which can be written in the form $L \cdot f$ for some $L \in R[\partial]$. Let us denote this submodule of F by $R[\partial] \cdot f$. It is often the case that we want to know something about this submodule, e.g., whether it contains an element with a certain desired property. However, it is not particularly handy to view it as a submodule of F, as the elements of F are typically inherently infinite objects such as formal power series with which we cannot easily do computations. We can fix this by considering the module homomorphism $\phi\colon R[\partial] \to F$ defined by $\phi(L) = L \cdot f$. By the homomorphism theorem, we have $R[\partial]/\operatorname{ann}(f) \cong R[\partial] \cdot f$, and therefore, computations in $R[\partial] \cdot f$ are equivalent to computations in $R[\partial]/\operatorname{ann}(f)$. In most of what follows, we will be doing computations in an Ore algebra $R[\partial]$ or a quotient $R[\partial]/I$ for some left-ideal I of $R[\partial]$ rather than computations with explicit “functions”.

Example 4.10 For $f = 1/(1 - \sqrt{x}) \in C[[x]]$ we have

$$(3f + x(x^2 - 1)f')' = -\tfrac{1}{2}(x + 1)f + \tfrac{1}{2}(x^2 - 4x + 5)f'.$$

The series f is annihilated by the operator $L = 2x(x - 1)D^2 + (5x - 1)D + 1 \in C(x)[D]$, and in $C(x)[D]/\langle L\rangle$ we have

$$D \cdot [3 + x(x^2 + 1)D] = [-\tfrac{1}{2}(x + 1) + \tfrac{1}{2}(x^2 - 4x + 5)D].$$

Note that the element $[1] \in C(x)[D]/\langle L\rangle$ plays the role of the function f which is annihilated by L. □

Left-$R[\partial]$-modules generalize the notion of D-modules introduced at the end of Sect. 3.2 and are sometimes also called ∂-*modules* for short. Whenever we say $R[\partial]$-module, we always mean a left module.

Proposition 4.6 suggests to restrict the attention to Ore algebras $K[\partial]$ where K is a field. While every Ore algebra $R[\partial]$ where R is an integral domain can be uniquely extended to an Ore algebra $\mathrm{Quot}(R)[\partial]$ (Exercise 5), not every $R[\partial]$-module admits a natural extension to a $\mathrm{Quot}(R)[\partial]$-module, so while the theory and algorithms are simpler for Ore algebras over fields, restricting the attention to these algebras is "with loss of generality".

Example 4.11

1. $C[[x]]$ is a $C[x][D]$-module but not a $C(x)[D]$-module, because not every element of $C[[x]]$ can be multiplied with any element of $C(x)$. However, $C((x))$ is a natural extension of $C[[x]]$ which is a $C(x)[D]$-module, and whenever $L \in C[x][D]$ is an annihilating operator of a series $f \in C[[x]] \subseteq C((x))$, then so is every element of the ideal generated by L in $C(x)[D]$. There is therefore no harm in working with $C(x)[D]$ instead of $C[x][D]$.
2. $C^{\mathbb{N}}$ is a $C[x][S]$-module but not a $C(x)[S]$-module, because we cannot meaningfully multiply a sequence with a rational function that has a pole at a nonnegative integer. It can happen that an operator L annihilates a sequence f, but not every $C(x)$-multiple of L does. For example, $L = (x - 5)$ annihilates the sequence $f : \mathbb{N} \to C$ with $f(5) = 1$ and $f(n) = 0$ for $n \neq 5$, but $\frac{1}{x-5}L = 1 \in C[x][S]$ does not. So unlike in the first example, if $L \in C[x][S]$ annihilates a sequence $f \in C^{\mathbb{N}}$, the ideal generated by L in $C(x)[S]$ may contain operators that do not annihilate f, and they may even belong to $C[x][S]$. □

When it is appropriate to work with a field, the arguments given in earlier chapters for D-finite closure properties can be easily lifted to the general setting. They reduce to linear algebra over K.

Theorem 4.12 *Let $K[\partial]$ be an Ore algebra over a field K, and let F be a $K[\partial]$-module.*

1. *$f \in F$ is D-finite if and only if the dimension of $K[\partial] \cdot f$ as a K-vector space is finite. If f is D-finite and L is a minimal element of* $\mathrm{ann}(f)$*, then* $\dim_K(K[\partial] \cdot f) = \mathrm{ord}(L)$.
2. *If $f \in F$ is D-finite with respect to $K[\partial]$ and annihilated by an operator of order at most r, then the same is true for $M \cdot f \in F$, for every $M \in K[\partial]$.*
3. *If $f, g \in F$ are D-finite with respect to $K[\partial]$ and annihilated by operators of orders at most r and s, respectively, then $f + g$ is D-finite as well and annihilated by an operator of order at most $r + s$.* □

Proof

1. "$\Rightarrow$": Let L be the monic minimal element of $\mathrm{ann}(f)$, and let $r = \mathrm{ord}(L)$. We show that $K[\partial] \cdot f$ is generated by $f, (\partial \cdot f), \dots, (\partial^{r-1} \cdot f)$. It suffices to show that every subspace generated by $f, (\partial \cdot f), \dots, (\partial^k \cdot f)$, for some $k \geq r$, is generated by $f, (\partial \cdot f), \dots, (\partial^{r-1} \cdot f)$, and this is easily seen by induction on k using that $\partial^k \cdot f = (\partial^k \cdot f) - \partial^{k-r} \cdot (L \cdot f) = (\partial^k - \partial^{k-r} L) \cdot f$ is contained in the subspace generated by $f, (\partial \cdot f), \dots, (\partial^{k-1} \cdot f)$, for any $k \geq r$.
   "$\Leftarrow$": If the dimension of $K[\partial] \cdot f$ is r, then any $r+1$ elements of $K[\partial] \cdot f$ must be linearly dependent over K. In particular, there will be $\ell_0, \dots, \ell_r \in K$, not all

zero, such that $\ell_0 f + \cdots + \ell_r(\partial^r \cdot f) = 0$, i.e., $\operatorname{ann}(f)$ contains the nonzero element $L = \ell_0 + \cdots + \ell_r \partial^r$ and hence f is D-finite.

For the claim about the dimension, note that the argument given above for "$\Rightarrow$" already implies that $\dim_K(K[\partial] \cdot f) \leq r$. If the dimension were smaller, then $f, \ldots, (\partial^{r-1} \cdot f)$ would be linearly dependent over K, and the linear dependence would give rise to a nonzero annihilating operator of order less than r, in contradiction to the minimality of L.

2. Let L be a minimal element of $\operatorname{ann}(f)$, and let $r = \operatorname{ord}(L)$. By part 1, the submodule $K[\partial] \cdot f$ of F is a K-vector space of dimension r. Since it is closed under ∂, it contains $M \cdot f$ and all its derivatives. Hence, the elements $M \cdot f, \ldots, \partial^r \cdot (M \cdot f)$ of $K[\partial] \cdot f$ are linearly dependent over K, i.e., there are $p_0, \ldots, p_r \in K$, not all zero, such that $(p_0 + \cdots + p_r \partial^r) \cdot (M \cdot f) = 0$, as claimed.
3. $f + g$ is an element of the submodule $(K[\partial] \cdot f) + (K[\partial] \cdot g) \subseteq F$. By part 1, this submodule is a K-vector space of dimension at most $r + s$, hence $(f + g), \ldots, \partial^{s+r} \cdot (f + s)$ must be linearly dependent, and the dependence gives rise to an annihilating operator for $f + g$. ■

We have seen in the previous chapters that D-finiteness is also preserved under multiplication (cf. Theorems 2.30 and 3.25). In order to lift this property to the general realm of Ore algebras, we must consider function spaces F that have a multiplication, and the multiplication must be compatible with the module structure. By a multiplication we mean a K-bilinear function

$$m\colon F \times F \to F, \qquad m(f, g) = fg,$$

i.e., a function which is additive in both arguments and satisfies $pm(f, g) = m(pf, g) = m(f, pg)$ for all $f, g \in F$ and all $p \in K$. It need not be commutative or associative, nor is it necessary to have a neutral element in F. But we do want to have a product rule that relates m to the action of ∂. More precisely, we will assume that there are $\alpha, \beta, \gamma \in K$ such that for all $f, g \in F$ we have

$$\partial \cdot m(f, g) = \alpha m(f, g) + \beta m(\partial \cdot f, g) + \beta m(f, \partial \cdot g) + \gamma m(\partial \cdot f, \partial \cdot g).$$

If f, g are D-finite, say $L \cdot f = M \cdot g = 0$ for some nonzero operators $L, M \in K[\partial]$, then every $\partial^n \cdot m(f, g)$ ($n \in \mathbb{N}$) belongs to the K-vector space generated by $m(\partial^i \cdot f, \partial^j \cdot g)$ for $i = 0, \ldots, \operatorname{ord}(L) - 1$ and $j = 0, \ldots, \operatorname{ord}(M) - 1$ in F. As this subspace has dimension at most $\operatorname{ord}(L)\operatorname{ord}(M)$, we find that $m(f, g), \ldots, \partial^{\operatorname{ord}(L)\operatorname{ord}(M)} \cdot m(f, g)$ are linearly dependent over K and thus $m(f, g)$ is D-finite and annihilated by an operator of order at most $\operatorname{ord}(L)\operatorname{ord}(M)$. The argument is always the same: a system of linear equations with more variables than equations must have a nontrivial solution.

It is worth noting that in the case of addition, all we need to know for computing an annihilating operator for $f + g$ are annihilating operators L and M of f and g. In fact, we do not need any f, g, F to begin with, but can start right away from an Ore algebra $K[\partial]$ and two nonzero elements L and M. We can then choose the module $F = (K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle)$ with the action $P \cdot ([v],[w]) = ([Pv],[Pw])$. Then for $f = ([1],[0])$ and $g = ([0],[1])$ we have $L \cdot f = M \cdot g = 0$, and since $\dim_K(F) = \operatorname{ord}(L) + \operatorname{ord}(M)$, we find that $f + g = ([1],[1])$ is annihilated by an operator of order (at most) $\operatorname{ord}(L) + \operatorname{ord}(M)$. This operator will be such that for every $K[\partial]$-module F and any elements $f, g \in F$ with $L \cdot f = M \cdot g = 0$, it annihilates $f + g$.

Also for multiplication, we do not need to know much about the module F or its multiplication function m. All that enters into the argument are the coefficients $\alpha, \beta, \gamma \in K$ that connect ∂ to m. Given two operators $L, M \in K[\partial]$, we can use the vector space tensor product $(K[\partial]/\langle L\rangle) \otimes_K (K[\partial]/\langle M\rangle)$ as the function space F. Recall from linear algebra that the tensor product of two K-vector spaces V, W consists of all finite K-linear combinations of the formal quantities $v \otimes w$ with $v \in V$ and $w \in W$, which satisfy the laws $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$, $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$ and $p(v \otimes w) = (pv) \otimes w = v \otimes (pw)$ for all $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ and $p \in K$. With the help of $\alpha, \beta, \gamma \in K$, we can turn the K-vector space $F = (K[\partial]/\langle L\rangle) \otimes_K (K[\partial]/\langle M\rangle)$ into a $K[\partial]$-module, by defining $\partial \cdot ([v] \otimes [w]) = \alpha([v] \otimes [w]) + \beta([\partial v] \otimes [w]) + \beta([v] \otimes [\partial w]) + \gamma([\partial v] \otimes [\partial w])$. The coefficients α, β, γ are not uniquely determined by $K[\partial]$ (Exercise 19), but also not completely arbitrary (Exercise 20).

Definition 4.13 Let $K[\partial]$ be an Ore algebra and let $L, M \in K[\partial]$ be nonzero.

1. Let $\alpha, \beta, \gamma \in K$ be such that the definition

$$\partial \cdot ([v] \otimes [w]) := \alpha([v] \otimes [w]) + \beta([\partial v] \otimes [w]) + \beta([v] \otimes [\partial w]) + \gamma([\partial v] \otimes [\partial w])$$

   for $v, w \in K[\partial]$ turns $F = (K[\partial]/\langle L\rangle) \otimes_K (K[\partial]/\langle M\rangle)$ into a $K[\partial]$-module. Then the unique monic minimal element of $\operatorname{ann}([1] \otimes [1])$ is called the *symmetric product* of L and M with respect to α, β, γ. It is denoted by $L \otimes M$.
2. With $\alpha, \beta, \gamma \in K$ as above we define $L^{\otimes 1} = L$ and $L^{\otimes (n+1)} = L \otimes L^{\otimes n}$ for $n \geq 1$, and call $L^{\otimes n}$ the nth *symmetric power* of L with respect to α, β, γ.
3. Now let $F = (K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle)$ and turn F into a $K[\partial]$-module by setting $\partial \cdot ([v],[w]) := ([\partial v],[\partial w])$ for all $v, w \in K[\partial]$. Let $s = ([1],[1])$. Then the unique monic minimal element of $\operatorname{ann}(s)$ is called the *symmetric sum* of L and M. It is denoted by $L \oplus M$. □

It is not hard to see that the symmetric sum and the symmetric product are commutative, i.e., we have $L \otimes M = M \otimes L$ and $L \oplus M = M \oplus L$ for all $M, L \in K[\partial]$. Furthermore, we have $1 \otimes M = 1$ and $1 \oplus M = M$ for all $M \in K[\partial]$, in agreement with the fact that we must have $0f = 0$ and $0 + f = f$ for any element f of any $K[\partial]$-module F. Finally, $\otimes$ and $\oplus$ are associative (Exercise 22), and we have the distributive law $L \otimes (M_1 \oplus M_2) = (L \otimes M_1) \oplus (L \otimes M_2)$ for $L, M_1, M_2 \in K[\partial]$ (Exercise 23). The Ore algebra $K[\partial]$ together with the operations $\oplus$ and $\otimes$ is a commutative semi-ring. It is not a ring because it lacks a notion of subtraction.

Example 4.14 Symmetric sums and products can be computed by linear algebra. For example, consider the Ore algebra $K[\partial]$ with $K = C(x)$, and with $\sigma, \delta\colon K \to K$ defined by $\sigma(p(x)) = p(x^2)$ and $\delta(p(x)) = 5p(x^2) - 5p(x)$ for all $p(x) \in K$. Let $L = \partial + x^2$ and $M = \partial^2 - x$.

1. We have

$$L \oplus M = \partial^3 + \tfrac{x^{12}+x^{11}-4x^{10}-4x^9-9x^8-9x^7+16x^6+16x^5+26x^4+26x^3-25x^2-25x+5}{x^4+x^3-4x^2-4x+1}\partial^2$$
$$- x^2\partial + \tfrac{-x^{13}-x^{12}+4x^{11}+4x^{10}+9x^9+9x^8-16x^7-21x^6-26x^5-x^4+25x^3}{x^4+x^3-4x^2-4x+1}.$$

This operator can be found as follows. First, apply successive powers of ∂ to the element $([1], [1])$ of the product space $K[\partial]/\langle L\rangle \times K[\partial]/\langle M\rangle$. Note that whenever an operator of order ≥ 1 appears in a first component, we can subtract from it a suitable left-multiple of L and replace it by a representative of order < 1. For the second component, any representative of order ≥ 2 can be replaced by a representative of order < 2 by adding a suitable left-multiple of M. In other words, every element of $K[\partial]/\langle L\rangle \times K[\partial]/\langle M\rangle$ is a K-linear combination of $([1], [0])$, $([0], [1])$, and $([0], [\partial])$. In particular,

$$\begin{aligned}
([1], [1]) &= ([1], [1]),\\
\partial \cdot ([1], [1]) &= ([-x^2], [\partial]),\\
\partial^2 \cdot ([1], [1]) &= ([x^6 - 5x^4 + 5x^2], [x]),\\
\partial^3 \cdot ([1], [1]) &= ([-x^{14} + 5x^{12} + 5x^{10} - 25x^8 - 10x^6 + 50x^4 - 25x^2],\\
&\qquad [x^2\partial + 5x^2 - 5x]).
\end{aligned}$$

Now we make an ansatz for an operator $P = p_0 + p_1\partial + p_2\partial^2 + p_3\partial^3$ and set up a linear system to enforce $P \cdot ([1], [1]) = ([0], [0])$. Coefficient comparison leads to

$$\begin{pmatrix} 1 & -x^2 & x^6-5x^4+5x^2 & -x^{14}+5x^{12}+5x^{10}-25x^8-10x^6+50x^4-25x^2 \\ 1 & 0 & x & 5x^2-5x \\ 0 & 1 & 0 & x^2 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{pmatrix} = 0$$

whose solution space is generated by the coefficient vector of the operator announced above.

2. For the choice $\alpha = 20$, $\beta = 5$, $\gamma = 1$, we have

$$\begin{aligned}
L \otimes M = \partial^2 &+ 10(x^4 - 4)\partial\\
&- (x^7 - 25x^6 - 5x^5 + 75x^4 - 5x^3 + 125x^2 + 25x - 400).
\end{aligned}$$

In order to find this operator, we find a linear relation among the elements $\partial^n \cdot (1 \otimes 1)$ $(n = 0, 1, 2)$ of the tensor product space $K[\partial]/\langle L\rangle \otimes_K K[\partial]/\langle M\rangle$. We have

$$\begin{aligned}
[1] \otimes [1] &= 1([1] \otimes [1]) + 0([1] \otimes [\partial]),\\
\partial \cdot ([1] \otimes [1]) &= 20([1] \otimes [1]) + 5([-x^2] \otimes [1])\\
&\quad + 5([1] \otimes [\partial]) + ([-x^2] \otimes [\partial])\\
&= (-5x^2 + 20)([1] \otimes [1]) + (5 - x^2)([1] \otimes [\partial]),\\
\partial^2 \cdot ([1] \otimes [1]) &= (x^7 + 25x^6 - 5x^5 - 125x^4 - 5x^3\\
&\quad - 75x^2 + 25x + 400)([1] \otimes [1])\\
&\quad - (10x^6 - 50x^4 - 40x^2 + 200)([1] \otimes [\partial]).
\end{aligned}$$

Now we make an ansatz for an operator $P = p_0 + p_1\partial + p_2\partial^2$ and set up a linear system to enforce $P \cdot ([1] \otimes [1]) = ([0] \otimes [0])$. Coefficient comparison leads to a linear system for p_0, p_1, p_2 whose solution space is generated by the coefficient vector of the operator announced above. □

Typically, we will not have a natural interest in the modules $(K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle)$ or $(K[\partial]/\langle L\rangle) \otimes_K (K[\partial]/\langle M\rangle)$, but we want to reason about elements of some other $K[\partial]$-modules F. For example, there might be two specific D-finite elements f, g of F for which we know annihilating operators $L, M \in K[\partial]$, and we might want to know an annihilating operator of their sum $f + g$. The point is that although $(K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle)$ may be different from F, we can be sure that the symmetric sum $L \oplus M$ will be an annihilating operator of $f + g$. The reason is that when L and M are annihilating operators of f and g, respectively, then we can define a module homomorphism

$$\phi\colon (K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle) \to F, \quad \phi([U], [V]) = (U \cdot f) + (V \cdot g),$$

and so if $P \in K[\partial]$ is an annihilating operator for $([1], [1])$, i.e., $P \cdot ([1], [1]) = 0$, then also $\phi(P \cdot ([1], [1])) = P \cdot \phi([1], [1]) = P \cdot (f + g) = 0$. The reasoning for multiplication is analogous, except that in this case F must also be a K-algebra, and α, β, γ must be chosen in such a way that they are compatible with the multiplication of F.

The symmetric sum and the symmetric product can thus be used to work in arbitrary $K[\partial]$-modules F, and they are oblivious to the particular F that we have in mind. A price we have to pay for this generality is that in general we cannot preserve minimality: even if L and M are the unique monic minimal operators annihilating f and g, respectively, the operators $L \oplus M$ and $L \otimes M$ are in general not minimal annihilating operators of $f + g$ and fg, respectively. As a counterexample, consider the case $g = -f$ and $M = L$. In this case, we have $L \oplus L = L$ (Exercise 21) while $f + g = 0$ is also annihilated by $1 \in K[\partial]$.

For the multiplication case, take for example $f = 1 + \exp(x)$, $g = 1 - \exp(x) \in C((x))$ and $L = M = D^2 - D$. Then we have $L \otimes M = D^3 - 3D^2 + 2D$ but $fg = 1 - \exp(2x)$ is also annihilated by $D^2 - 2D$.

Exercises

1. Let $\sigma, \delta\colon C[x] \to C[x]$ be defined by $\sigma(p(x)) = p(x+1)$ for $p \in C[x]$ and $\delta(p(x)) = p(x+1) - p(x)$. Show that δ is a σ-derivation.

2. Write the elements $(x+\partial^2)(1-2\partial+x\partial^2)$ and $1-\partial(x+3x^2)+(x+1)\partial^2(x-1)$ of $K[\partial]$ in the standard form $p_0 + p_1\partial + p_2\partial^2 + \cdots$, given that

a. $\sigma = \mathrm{id}$ and $\delta = \frac{d}{dx}$,

b. $\sigma(p(x)) = p(x+1)$ and $\delta = 0$,

c. $\sigma(p(x)) = p(x^2)$ and $\delta(p(x)) = 5p(x^2) - 5p(x)$.

3⋆. Show that $D^n x^k = \sum_{i\ge 0} \binom{n}{i} k^{\underline{i}} x^{k-i} D^{n-i}$ for all $n, k \in \mathbb{N}$.

4⋆. Let R be an integral domain, $\sigma\colon R \to R$ be an endomorphism, and $\delta\colon R \to R$ be a σ-derivation. For $m \in \mathbb{N}$ and $p \in R$, we use the notation $\sigma^{\overline{m}}(p) = p\sigma(p)\cdots\sigma^{m-1}(p)$. Show that we have

$$\delta(\sigma^{\overline{m}}(p)) = \delta\big(p + \sigma(p) + \cdots + \sigma^{m-1}(p)\big)\sigma^{\overline{m-1}}(\sigma(p))$$

for all $m \in \mathbb{N}$ and all $p \in R$. This formula generalizes the formula $D(a^n) = na^{n-1}D(a)$ from Exercise 9 in Sect. 3.2.

5. Let R be an integral domain, $\sigma\colon R \to R$ be an injective endomorphism, and $\delta\colon R \to R$ be a σ-derivation. Show that for $K = \mathrm{Quot}(R)$, there exists exactly one endomorphism $\bar\sigma\colon K \to K$ and exactly one $\bar\sigma$-derivation $\bar\delta\colon K \to K$ with $\bar\sigma|_R = \sigma$ and $\bar\delta|_R = \delta$.

6. Show that in a Laurent Ore polynomial ring $R[\partial, \partial^{-1}]$, we must have $\partial^{-1}\sigma(p) = p\partial^{-1} - \partial^{-1}\delta(p)\partial^{-1}$ for all $p \in R$.

7. Let $L \in K[\partial]$ and $m, y \in K$. Prove or disprove:

a. $L \cdot y = m \Rightarrow (L - m) \cdot y = 0$.

b. $(L - m) \cdot y = 0 \Rightarrow L \cdot y = m$.

8. Let $\sigma\colon K \to K$ be an endomorphism and $\delta\colon K \to K$ be a σ-derivation. Show:

a. If $\sigma \neq \mathrm{id}$, then there exists an element $u \in K$ such that $\delta(q) = u(\sigma(q) - q)$ for all $q \in K$.

b. If $\delta \neq 0$, then there exists an element $u \in K$ such that $\sigma(q) = u\delta(q) + q$ for all $q \in K$.

9. Prove or disprove: If $\sigma\colon R \to R$ is an endomorphism and $\delta\colon R \to R$ is a σ-derivation, then $\sigma \circ \delta = \delta \circ \sigma$.

10. Let R be an integral domain, and $\sigma \neq \mathrm{id}$ or $\delta \neq 0$. Suppose that σ is injective. Let $Z(R[\partial]) = \{\, p \in R[\partial] \mid \forall\, q \in R[\partial] : pq = qp \,\}$ be the centralizer of $R[\partial]$, and consider $\mathrm{Const}(R) \subseteq R \subseteq R[\partial]$. Prove or disprove:

a. $\mathrm{Const}(R) \subseteq Z(R[\partial])$

b. $Z(R[\partial]) \subseteq \mathrm{Const}(R)$

11. Determine the unique monic minimal annihilating operator of $\frac{x+1}{x-1} \in C(x)$ **a.** in $C(x)[D]$; **b.** in $C(x)[S]$; **c.** in $C(x)[M_2]$.

12. Is the commutative polynomial ring $C(x)[Y]$ an Ore algebra? Can we view $F = C((x))$ as a $C(x)[Y]$-module with the action $Y^i \cdot f = f^i$, so that a series is D-finite with respect to $C(x)[Y]$ if and only if it is algebraic?

13⋆. Show that $\exp(x)$ is not D-finite with respect to $C(x)[M_2]$.

14. Show that $f(x) = \sum_{n=0}^{\infty} q^{n^2} x^n$ with q not a root of unity is D-finite with respect to the q-shift operator but not with respect to the usual derivation.

Hint: You may use without proof that for any pairwise distinct $\phi_1, \ldots, \phi_r \in C$ the sequences $(\phi_i^n)_{n=0}^{\infty}$ are linearly independent over $C(n)$.

15. Prove or disprove: For all $L, M \in C(x)[D]$ there exists $\tilde{M} \in C(x)[D]$ such that $LM = \tilde{M}L$.

16. Show that a sequence is D-finite with respect to $C[x][S]$ if and only if it is D-finite with respect to $C[x][\Delta]$.

17⋆. Let $R[\partial]$ be an Ore algebra over a commutative ring R. Show that for all $L, M \in R[\partial] \setminus \{0\}$ we have $\mathrm{ord}(LM) = \mathrm{ord}(L) + \mathrm{ord}(M)$ if and only if R is an integral domain and σ is injective.

18⋆. For $F = C((x))$, the Hadamard product $m\colon F \times F \to F$, $m(f, g) = f \odot g$ is a C-bilinear function. Show that there are no $\alpha, \beta, \gamma \in C$ such that for all $f, g \in C((x))$ we have $m(f, g)' = \alpha m(f, g) + \beta m(f', g) + \beta m(f, g') + \gamma(f', g')$.

19. Let F be a $K[\partial]$-module and $m\colon F \times F \to F$ a bilinear map such that there are $\alpha, \beta, \gamma \in K$ with $\partial \cdot m(f, g) = \alpha m(f, g) + \beta m(\partial \cdot f, g) + \beta m(f, \partial \cdot g) + \gamma m(\partial \cdot f, \partial \cdot g)$ for all $f, g \in F$. Let $q \in K \setminus \{0\}$ and define $\tilde{m}\colon F \times F \to F$ by $\tilde{m}(f, g) := q m(f, g)$. Determine $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma} \in K$ such that $\partial \cdot \tilde{m}(f, g) = \alpha \tilde{m}(f, g) + \beta \tilde{m}(\partial \cdot f, g) + \beta \tilde{m}(f, \partial \cdot g) + \gamma \tilde{m}(\partial \cdot f, \partial \cdot g)$ for all $f, g \in F$.

20⋆⋆. Show that if $\alpha, \beta, \gamma \in K$ are such that the symmetric product with respect to α, β, γ is well-defined for an Ore algebra $K[\partial]$, then $(p - \sigma(p))\alpha + \delta(p)(\beta - 1) = (p - \sigma(p))\beta + \delta(p) = 0$ for all $p \in K$.

21. Show that for all $M, L \in K[\partial]$ we have $L \oplus M \in \langle L \rangle \cap \langle M \rangle$. Conclude that $L \oplus L = L$ for all monic $L \in K[\partial]$.

22. Show that the operations $\otimes, \oplus\colon K[\partial] \times K[\partial] \to K[\partial]$ are associative.

23. Let $\alpha, \beta, \gamma \in K$ be such that the symmetric product with respect to α, β, γ is defined for an Ore algebra $K[\partial]$. Show that for all $M, L_1, L_2 \in K[\partial]$ we have $M \otimes (L_1 \oplus L_2) = (M \otimes L_1) \oplus (M \otimes L_2)$.

24.** (Stavros Garoufalidis and Christoph Koutschan) Let $C(q)$ be a field of rational functions over C, consider the Ore algebra $C(q)(x)[Q]$ with $\sigma(p(x)) = p(qx)$ for $p \in C(q)(x)$ and $\delta = 0$, and let $F = C(q)^{\mathbb{N}}$ be the set of sequences in $C(q)$. The set F becomes a $C(q)(x)[Q]$-module by setting $x \cdot (a_n(q))_{n=0}^{\infty} = (q^n a_n(q))_{n=0}^{\infty}$ and $Q \cdot (a_n(q))_{n=0}^{\infty} = (a_{n+1}(q))_{n=0}^{\infty}$. Let $\omega \in C$ be a root of unity. Show that if $(a_n(q))_{n=0}^{\infty}$ is D-finite with respect to the action of $C(q)(x)[Q]$, then so is $(a_n(\omega q))_{n=0}^{\infty}$.

Hint: Show that for any integer $k \geq 2$, there is an annihilating operator of $(a_n(q))_{n=0}^{\infty}$ with polynomial coefficients in which all exponents of x are divisible by k.

25. Let the Ore algebra $C(x)[M_2]$ act on $C((x))$ via $M_2 \cdot f(x) = f(x^2)$ for $f \in C((x))$. Suppose that $f, g \in C((x))$ are such that $(M_2^2 + xM_2 + x^2) \cdot f = (M_2^2 - xM_2 + x^2) \cdot g = 0$. Compute annihilating operators for $f + g$ and fg.

26. Let $K[\partial]$ be an Ore algebra and F be a $K[\partial]$-module. Let $L \in K[\partial] \setminus \{0\}$ and let $f, g \in F$ be such that $L \cdot f = g$. Prove or disprove:

a. If f is D-finite, then so is g.

b. If g is D-finite, then so is f.

27. (Clemens Raab) Let F be a $K[\partial]$-module and $m\colon F \times F \to F$ be a bilinear map with $m(f, g) = m(g, f)$ for all $f, g \in F$. Let $L, M \in K[\partial]$ be such that $L \cdot f = 0 \Rightarrow M \cdot m(f, f) = 0$ for all $f \in F$. Show that then we even have $M \cdot m(f_1, f_2) = 0$ for any two $f_1, f_2 \in F$ with $L \cdot f_1 = L \cdot f_2 = 0$.

References

General expositions on the theory of noncommutative rings can be found in [186, 303, 316]. As remarked in the text, the rings we consider here are, in a way, only slightly noncommutative, which makes it possible to handle them without first going through a general course on noncommutative rings. Ore algebras were introduced and first studied by Ore [344]. He already drew his motivation from differential and recurrence operators. Bronstein and Petkovšek introduced Ore algebras into computer algebra in their tutorial paper [115].

It has been remarked that the orders of $L \oplus M$ and $L \otimes M$ are in general larger than necessary. At the same time, it can be shown that the orders do not overshoot if the module F is sufficiently large, in the following sense: if $L, M \in C(x)[D]$ are such that $\dim_C V(L) = \operatorname{ord}(L)$ and $\dim_C V(M) = \operatorname{ord}(M)$, then $\dim_C V(L \oplus M) = \operatorname{ord}(L \oplus M)$ and $V(L \oplus M) = V(L) + V(M)$. Moreover, if F is even a differential ring, then $\dim_C V(L \otimes M) = \operatorname{ord}(L \otimes M)$ and $V(L \otimes M)$ is the C-vector space generated by $\{ fg : f \in V(L), g \in V(M)\}$ in F. Proofs can be found in a paper of

Singer [406] or, using more abstract constructions, in the book of van der Put and Singer [441].

The multiplication algorithm stated in this section is straightforward. More sophisticated algorithms are known, at least for the differential case. Benoit, Bostan, and van der Hoeven [54] showed that the product of two elements of $C[x][D]$ whose degrees in x and D are d and r, respectively, can be computed with $\mathrm{O}^{\sim}(\min(d,r)^{\omega-2}dr)$ operations in C, where ω is the exponent of matrix multiplication (cf. Sect. 1.4). Bostan, Chyzak, and Le Roux [84] showed some sort of converse: the product of two $n \times n$ matrices with coefficients C can be computed with a number of operations in C that does not exceed the number of operations in C needed to compute the a certain fixed number of products of two elements of $C[x][D]$ whose degrees in both x and D are bounded by n.

4.2 Common Right Divisors and Left Multiples

In this section, we consider an arbitrary Ore algebra $K[\partial]$ over a field K. We assume throughout that σ is injective. We have already observed that despite being non-commutative, the Ore algebra $K[\partial]$ has some similarities with the commutative polynomial ring $C[x]$. For example, the order in $K[\partial]$ plays the role of the degree in $C[x]$. Thanks to the degree function, $C[x]$ is a Euclidean domain, and we will now see that $K[\partial]$ is a right-Euclidean domain.

Theorem 4.15 *For every $U, V \in K[\partial]$ with $v \neq 0$ there exists a unique pair $(Q, R) \in K[\partial]^2$ such that $U = QV + R$ and* $\operatorname{ord}(R) < \operatorname{ord}(V)$. □

Proof There clearly exist Q, R with $U = QV + R$, for example $Q = 0$, $R = U$ is a valid choice. Among all pairs (Q, R) with $U = QV + R$, select one for which $\operatorname{ord}(R)$ is minimal. We show that $\operatorname{ord}(R) < \operatorname{ord}(V)$. If we had $\operatorname{ord}(R) \geq \operatorname{ord}(V)$, there is a $c \in K$ such that $\operatorname{ord}(R - c\partial^{\operatorname{ord}(R)-\operatorname{ord}(V)}V) < \operatorname{ord}(R)$, and for $R' = R - c\partial^{\operatorname{ord}(R)-\operatorname{ord}(V)}V$ and $Q' = Q + c\partial^{\operatorname{ord}(R)-\operatorname{ord}(V)}$ we have $U = Q'V + R'$, in contradiction to the minimality assumption on R.

We have thus shown that a pair (Q, R) with $U = QV + R$ and $\operatorname{ord}(R) < \operatorname{ord}(V)$ always exists. For the uniqueness, suppose there is another pair (Q', R') with $U = Q'V + R'$ and $\operatorname{ord}(R') < \operatorname{ord}(V)$. Then $(Q - Q')V = R' - R$. The left hand side has order $\operatorname{ord}(Q - Q') + \operatorname{ord}(V)$, while the order of the right hand side is strictly less than $\operatorname{ord}(V)$. Therefore $\operatorname{ord}(Q - Q') < 0$, which means $Q = Q'$. But then $0 = (Q - Q')V = R' - R$ also implies $R' = R$. ■

Definition 4.16 Let $U, V \in K[\partial]$, $V \neq 0$, and let $Q, R \in K[\partial]$ be as in Theorem 4.15. Then $\operatorname{rquo}(U, V) := Q$ is called the *right quotient* and $\operatorname{rrem}(U, V) := R$ is called the *right remainder* of U with respect to V. If $R = 0$, we say that V is a *right factor* or *right divisor* of U and that U is a *left multiple* of V. □

Given two elements $U, V \in K[\partial]$, we can compute the right quotient and the right remainder in very much the same way as in the commutative case. The proof of Theorem 4.15 translates into the following algorithm.

Algorithm 4.17
Input: $U, V \in K[\partial]$ *with* $V \neq 0$.
Output: $\operatorname{rquo}(U, V)$ *and* $\operatorname{rrem}(U, V)$.

Let $Q = 0$ *and* $R = U$.
while $\operatorname{ord}(R) > \operatorname{ord}(V)$, *do*
  $c = \frac{\operatorname{lc}(R)}{\sigma^{\operatorname{ord}(R)-\operatorname{ord}(V)}(\operatorname{lc}(V))}$
  $R = R - c\partial^{\operatorname{ord}(R)-\operatorname{ord}(V)}V$
  $Q = Q + c\partial^{\operatorname{ord}(R)-\operatorname{ord}(V)}$
Return (Q, R).

Example 4.18

1. For $U = (3x+5)D^3 - (2x+1)D^2 + (2x-3)D + (3x+1)$ and $V = (x+2)D - (3x+5) \in C(x)[D]$ the algorithm yields

$$\operatorname{rquo}(U, V) = \frac{3x+5}{x+2}D^2 + \frac{7x^2+19x+13}{(x+2)^2}D + \frac{23x^3+108x^2+177x+100}{(x+2)^3},$$
$$\operatorname{rrem}(U, V) = \frac{72x^4+479x^3+1212x^2+1374x+586}{(x+2)^3}.$$

   It can be seen that $\operatorname{ord}(\operatorname{rrem}(U, V)) = 0 < 1 = \operatorname{ord}(V)$, and it can be checked that $U = \operatorname{rquo}(U, V)V + \operatorname{rrem}(U, V)$.
2. For $U = (3x+5)S^3 - (2x+1)S^2 + (2x-3)S + (3x+1)$ and $V = (x+2)S - (3x+5) \in C(x)[S]$ the algorithm yields

$$\operatorname{rquo}(U, V) = \frac{3x+5}{x+4}S^2 + \frac{7x^2+39x+51}{(x+3)(x+4)}S + \frac{23x^3+184x^2+468x+372}{(x+2)(x+3)(x+4)},$$
$$\operatorname{rrem}(U, V) = \frac{72x^4+695x^3+2411x^2+3554x+1884}{(x+2)(x+3)(x+4)}.$$

   Again it can be seen that $\operatorname{ord}(\operatorname{rrem}(U, V)) = 0 < 1 = \operatorname{ord}(V)$, and it can be checked that $U = \operatorname{rquo}(U, V)V + \operatorname{rrem}(U, V)$. Note that although U, V have the same coefficients as before, the results are not the same. The coefficients of $\operatorname{rquo}(U, V)$, $\operatorname{rrem}(U, V)$ depend on the arithmetic of $K[\partial]$, which is governed by σ and δ. □

Definition 4.19 Let $U, V \in K[\partial]$, not both zero.

1. If $G \in K[\partial]$ is a right divisor of both U and V, it is called a *common right divisor* of U and V.

2. A common right divisor G of U and V is called a *greatest common right divisor* if it is monic and a right divisor of any other common right divisor.
3. If $M \in K[\partial]$ is a left multiple of both U and V, it is called a *common left multiple* of U and V.
4. A common left multiple M of U and V is called a *least common left multiple* if it is monic and a right divisor of any other common left multiple. □

It is easy to show that for any pair $(U, V) \in K[\partial]^2 \setminus \{(0, 0)\}$ there is at most one greatest common right divisor and at most one least common left multiple (Exercise 2). We denote these by $\operatorname{gcrd}(U, V)$ and $\operatorname{lclm}(U, V)$, respectively. We further define $\operatorname{gcrd}(0, 0) = 0$ and $\operatorname{lclm}(0, 0) = 0$.

Like in the commutative case, the existence of a greatest common right divisor follows from the correctness of the Euclidean algorithm, which happens to apply literally in the same way to Ore algebras. Also the extended Euclidean algorithm, which in addition to $\operatorname{gcrd}(U, V)$ computes $S, T \in K[\partial]$ such that $\operatorname{gcrd}(U, V) = SU + TV$, works for arbitrary Ore algebras $K[\partial]$.

Algorithm 4.20 *(Extended Euclidean Algorithm)*
Input: $U, V \in K[\partial]$*, not both zero.*
Output: $\operatorname{gcrd}(U, V)$ *and* $S, T \in K[\partial]$ *such that* $\operatorname{gcrd}(U, V) = SU + TV$.

Let $(G, S, T, G', S', T') = (U, 1, 0, V, 0, 1)$.
while $G' \neq 0$ *do*
    $Q = \operatorname{rquo}(G, G')$
    $(G, S, T, G', S', T') = (G', S', T', G - QG', S - QS', T - QT')$
Return $(\operatorname{lc}(G)^{-1}G, \operatorname{lc}(G)^{-1}S, \operatorname{lc}(G)^{-1}T)$.

Theorem 4.21 *Algorithm 4.20 is correct and terminates. In particular:*

1. *Any two elements* $U, V \in K[\partial]$ *with* $(U, V) \neq (0, 0)$ *have a greatest common right divisor* $\operatorname{gcrd}(U, V)$.
2. *For any* $U, V \in K[\partial]$ *with* $(U, V) \neq (0, 0)$ *there exist* $S, T \in K[\partial]$ *and* $\operatorname{gcrd}(U, V) = SU + TV$.
3. *If* $\operatorname{ord}(U) \geq \operatorname{ord}(V) \geq 0$ *and* $\operatorname{lc}(V)U \neq \operatorname{lc}(U)V$*, then for the pair* $(S, T) \in K[\partial]^2$ *computed by Algorithm 4.20 we have* $\operatorname{ord}(S) < \operatorname{ord}(V) - \operatorname{ord}(G)$ *and* $\operatorname{ord}(T) < \operatorname{ord}(U) - \operatorname{ord}(G)$.
4. *For any* $U, V \in K[\partial]$ *with* $(U, V) \neq (0, 0)$ *there exists at most one pair* $(S, T) \in K[\partial]^2$ *with* $\operatorname{gcrd}(U, V) = SU + TV$ *and* $\operatorname{ord}(S) < \operatorname{ord}(V) - \operatorname{ord}(G)$ *and* $\operatorname{ord}(T) < \operatorname{ord}(U) - \operatorname{ord}(G)$. □

Proof Termination is clear because $G - QG' = \operatorname{rrem}(G, G')$ implies that the order of G' decreases in every iteration, and since it is a natural number, it cannot decrease infinitely often. For the correctness, let $C(A, B) \subseteq K[\partial]$ denote the set of common right divisors of $A, B \in K[\partial]$. We then have $C(A, B) = C(B, A - QB)$ for every $Q \in K[\partial]$, because if D is a common right divisor of A and B, say $A = \tilde{A}D$ and $B = \tilde{B}D$ for some $\tilde{A}, \tilde{B} \in K[\partial]$, then $A - QB = (\tilde{Q} - Q\tilde{B})D$, so D is a common right divisor of B and $A - QB$. This shows $C(A, B) \subseteq C(B, A - QB)$, and the other inclusion follows by symmetry (replace Q by $-Q$).

We have thus shown that $C(U, V) = C(G, G')$ at the end of every iteration. Upon termination, we have $G' = 0$, and since $C(G, 0)$ contains exactly the right divisors of G, the monic element $\operatorname{lc}(G)^{-1}G$ must be the greatest common right divisor of U and V. For the claim about S and T, observe first that we have $G = SU + TV$ and $G' = S'U + T'V$ at the beginning, after every iteration of the while loop, and therefore right after the while loop.

This proves the correctness of the algorithm. Parts 1 and 2 of the theorem follow immediately. For part 3, consider first the case when $\operatorname{ord}(U) > \operatorname{ord}(V)$ and let S, T be as computed by Algorithm 4.20. Define $(G_0, S_0, T_0) = (U, 1, 0)$, and let (G_k, S_k, T_k) be the values of G, S, T at the end of the kth iteration ($k = 1, 2, \ldots$). If Q_k denotes the value of Q in the kth iteration, we have $Q_k = \operatorname{rquo}(G_{k-1}, G_k)$ for all $k \geq 1$, which implies $\operatorname{ord}(Q_k) = \operatorname{ord}(G_{k-1}) - \operatorname{ord}(G_k)$ for all $k \geq 1$. Therefore $\operatorname{ord}(G_k) = \operatorname{ord}(G_1) - \sum_{i=1}^{k} \operatorname{ord}(Q_i)$ for all $k \geq 1$. By the definition of G_k and the assumption $\operatorname{ord}(U) > \operatorname{ord}(V)$, we have $\operatorname{ord}(Q_k) > 0$ for all $k \geq 1$. Therefore, from $S_{k+1} = S_{k-1} - Q_k S_k = S_{k-1} - Q_k(S_{k-2} + Q_{k-1}S_{k-1})$ it follows that $\operatorname{ord}(S_{k+1}) = \operatorname{ord}(Q_k) + \operatorname{ord}(S_k)$ for all $k \geq 2$. Taking also into account that $S_2 = S_0 - Q_1 S_1 = 1$, we obtain $\operatorname{ord}(S_k) = \sum_{i=2}^{k-1} \operatorname{ord}(Q_i)$.

Suppose now that the algorithm terminates after the kth iteration, so that $G_k = G = \operatorname{gcrd}(U, V)$, $S_k = S$, $T_k = T$. Because of the assumption $\operatorname{ord}(U) > \operatorname{ord}(V) \geq 0$, we must have $k \geq 2$. Therefore, $\operatorname{ord}(G) = \operatorname{ord}(G_1) - \sum_{i=1}^{k} \operatorname{ord}(Q_i) < \operatorname{ord}(V) - \sum_{i=2}^{k-1} \operatorname{ord}(Q_i) = \operatorname{ord}(V) - \operatorname{ord}(S)$, so $\operatorname{ord}(S) < \operatorname{ord}(V) - \operatorname{ord}(G)$. Moreover, since $\operatorname{ord}(G) \leq \operatorname{ord}(V) < \operatorname{ord}(U)$ and we must have $S \neq 0$ when $k \geq 2$, the equation $G = SU + TV$ implies $\operatorname{ord}(S) + \operatorname{ord}(U) = \operatorname{ord}(T) + \operatorname{ord}(V)$, from which we obtain $\operatorname{ord}(T) = \operatorname{ord}(U) + \operatorname{ord}(S) - \operatorname{ord}(V) < \operatorname{ord}(U) - \operatorname{ord}(G)$. This completes the proof of the order bounds for S and T in the case $\operatorname{ord}(U) > \operatorname{ord}(V)$.

For the case $\operatorname{ord}(U) = \operatorname{ord}(V)$, we have $G_0 = U$, $G_1 = V$, $G_2 = V - \frac{\operatorname{lc}(V)}{\operatorname{lc}(U)} U$. The assumption on U and V ensures $G_2 \neq 0$ and $\operatorname{ord}(G_2) < \operatorname{ord}(V)$. We can therefore apply the previous argument with V and G_2 in place of U and V and obtain $S', T' \in K[\partial]$ with $G = S'V + T'G_2 = S'V + T'(V - \frac{\operatorname{lc}(V)}{\operatorname{lc}(U)} U) = (S' + T')V - T' \frac{\operatorname{lc}(U)}{\operatorname{lc}(V)} U$ and $\operatorname{ord}(S') < \operatorname{ord}(V) - \operatorname{ord}(G)$ and $\operatorname{ord}(T') < \operatorname{ord}(G_2) - \operatorname{ord}(G)$. Algorithm 4.20 applied to U and V will therefore give $S = T' \frac{\operatorname{lc}(U)}{\operatorname{lc}(V)}$ and $T = S' + T'$, and for these we have $\operatorname{ord}(S) = \operatorname{ord}(T') < \operatorname{ord}(G_2) - \operatorname{ord}(G) \leq \operatorname{ord}(V) - \operatorname{ord}(G)$ and $\operatorname{ord}(T) \leq \max(\operatorname{ord}(S'), \operatorname{ord}(T')) < \operatorname{ord}(V) - \operatorname{ord}(G) = \operatorname{ord}(U) - \operatorname{ord}(G)$.

The proof of part 4 is Exercise 6. ■

Example 4.22

1. In $C(x)[D]$, consider the operators

$$U = (x - 1)D^5 + 5D^4,$$

$$V = (x - 1)D^3 + (6 - 3x)D^2 + (27x^2 + 9x - 42)D + (117 - 54x).$$

For the sequence of successive remainders, we have $G_0 = U$, $G_1 = V$ and then

$$G_2 = \operatorname{rrem}(G_0, G_1) = -162(x^2-1)D^2 - 81(9x^3+12x^2-11x-18)D - 81(18x^2-21x-41),$$

$$G_3 = \operatorname{rrem}(G_1, G_2) = \frac{27}{4}(3x+4)(x+2)(x-1)D - \frac{27(3x+4)(2x^2-x-7)}{4(x+1)},$$

$$G_4 = \operatorname{rrem}(G_2, G_3) = 0.$$

It follows that

$$\operatorname{gcrd}(U, V) = \operatorname{lc}(G_3)^{-1}G_3 = D - \frac{2x^2-x-7}{(x+2)(x+1)(x-1)}.$$

2. In $C(x)[S]$, consider the operators

$$U = S^7 + 5S^6 + 9S^5 + 5S^4 - 5S^3 - 9S^2 - 5S - 1,$$
$$V = (x+5)S^5 + 6S^4 - 6S^3 - 2(x-1)S^2 - (x+19)S + 2(x+6).$$

For the sequence of successive remainders, we have $G_0 = U$, $G_1 = V$ and then

$$\begin{aligned}
G_2 &= \operatorname{rrem}(G_0, G_1)\\
&= +\frac{(x+4)(7x+27)}{(x+6)(x+7)}S^4 + \frac{2(3x^2+37x+102)}{(x+6)(x+7)}S^3 + \frac{2(x+5)(6x+1)}{(x+6)(x+7)}S^2\\
&\quad - \frac{2(3x^2-13x-148)}{(x+6)(x+7)}S - \frac{19x+103}{x+7},\\
G_3 &= \operatorname{rrem}(G_1, G_2)\\
&= -\frac{16(x+3)(x+7)(3x+11)}{(7x+27)(7x+34)}S^3 + \frac{16(x+7)(x^2-12x-58)}{(7x+27)(7x+34)}S^2\\
&\quad + \frac{16(x+7)(3x^2+40x+103)}{(7x+27)(7x+34)}S - \frac{16(x+2)(x+6)(x+7)}{(7x+27)(7x+34)},\\
G_4 &= \operatorname{rrem}(G_2, G_3)\\
&= \frac{2(x+2)(2x+7)(7x+27)(7x+34)}{(x+6)(x+7)(3x+11)(3x+14)}S^2\\
&\quad + \frac{20(x+4)(7x+27)(7x+34)}{(x+6)(x+7)(3x+11)(3x+14)}S - \frac{2(2x+9)(7x+27)(7x+34)}{(x+7)(3x+11)(3x+14)},\\
G_5 &= \operatorname{rrem}(G_3, G_4) = 0.
\end{aligned}$$

It follows that

$$\operatorname{gcrd}(U, V) = \operatorname{lc}(g_4)^{-1} g_4 = S^2 + \frac{10(x+4)}{(x+2)(2x+7)} S - \frac{(2x+9)(x+6)}{(2x+7)(x+2)}.$$

□

The example illustrates a phenomenon that also appears in the commutative case: the intermediate successive remainders have much larger coefficients than the final result. Since we need them only up to nonzero K-multiples, it is a good idea to introduce an additional instruction $(G, S, T) = (\operatorname{lt}(G)^{-1}G, \operatorname{lt}(G)^{-1}S, \operatorname{lt}(G)^{-1}T)$ at the end of the loop body in order to clear useless common K-factors that blow up the coefficients.

The example also illustrates a phenomenon that does not appear in the commutative case: the coefficients of the greatest common right divisor can be larger than those of the input. In the case of integers or univariate commutative polynomial rings over a field, there is a lemma by Gauss which says that this cannot happen, but as the example above shows, there is no natural counterpart of this lemma for $K[\partial]$.

In order to get a bound on the degree of the coefficients in the greatest common right divisor, we translate the question into linear algebra. It suffices to consider $U, V \in K[\partial]$ which are both nonzero and such that $\operatorname{lc}(V)U \neq \operatorname{lc}(U)V$ (otherwise the greatest common right divisor is obvious). Under these assumptions, we know from Theorem 4.21 that $\operatorname{gcrd}(U, V)$ can be written as $SU + TV$ for certain $S, T \in K[\partial]$ with $\operatorname{ord}(S) < \operatorname{ord}(V)$ and $\operatorname{ord}(T) < \operatorname{ord}(U)$. Since we know $r_V := \operatorname{ord}(V)$ and $r_U := \operatorname{ord}(U)$ when we know U and V, we can make an ansatz $S = s_0 + s_1\partial + \cdots + s_{r_V-1}\partial^{r_V-1}$ and $T = t_0 + t_1\partial + \cdots + t_{r_U-1}\partial^{r_U-1}$ with undetermined coefficients $s_0, \ldots, s_{r_V-1}, t_0, \ldots, t_{r_U-1} \in K$. If we write $\operatorname{gcrd}(U, V) = g_0 + g_1\partial + \cdots + g_{r_U+r_V-1}\partial^{r_U+r_V-1}$ for the coefficients of the greatest common right divisor of U and V, then we have the equation

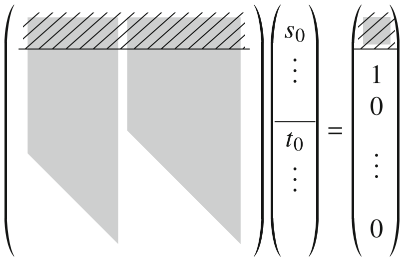
$$\operatorname{Syl}(U, V) \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{r_U-1} \\ t_0 \\ \vdots \\ t_{r_V-1} \end{pmatrix} = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ g_{r_U+r_V-1} \end{pmatrix}$$

where $\operatorname{Syl}(U, V) \in K^{(r_U+r_V)\times(r_U+r_V)}$ is the matrix whose first r_V columns are the coefficient vectors of $U, \partial U, \ldots, \partial^{r_V-1}U$ and whose last r_U columns are the coefficient vectors of $V, \partial V, \ldots, \partial^{r_U-1}V$. This matrix is called the *Sylvester matrix* for $U, V \in K[\partial]$. Its determinant is called the *resultant* of $U, V \in K[\partial]$ and is denoted by $\operatorname{res}(U, V)$. If the resultant is nonzero, we find a solution

$(s_0, \ldots, s_{r_U-1}, t_0, \ldots, t_{r_V-1})$ for any right hand side $(g_0, \ldots, g_{r_U+r_V-1})$, in particular for the right hand side $(1, 0, \ldots, 0)$. This means that in this case, we have $1 = SU + TV$ for some $S, T \in K[\partial]$, which implies that $\gcd(U, V) = 1$, because every common right divisor of U and V must also be a right divisor of $SU + TV$, no matter what S and T are, and since 1 obviously does not have any nontrivial right divisor, U and V cannot have a nontrivial common right divisor. We say that they are *right coprime.*

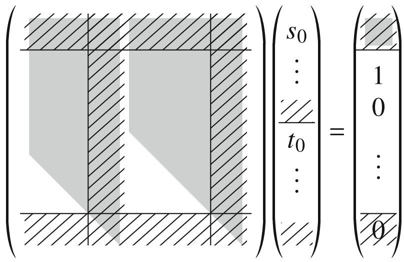
Conversely, if U and V are right coprime, then $SU + TV = 1$ for some $S, T \in K[\partial]$ with $\operatorname{ord}(S) < r_V$ and $\operatorname{ord}(T) < r_U$, and consequently $\partial^i SU + \partial^i TV = \partial^i$ for every $i \in \mathbb{N}$. From Theorem 4.28 below, it follows that there also are $S', T' \in K[\partial]$ with $\operatorname{ord}(S') \leq r_V$ and $S'U + T'V = 0$. Therefore, $\operatorname{rrem}(\partial^i S, S')U + (\partial^i T - \operatorname{rquo}(\partial^i S, S')T')V = \partial^i$ for every $i = 0, \ldots, r_V + r_U - 1$. Because of $\operatorname{ord}(\operatorname{rrem}(\partial^i S, S')) < r_V$ and $\operatorname{ord}(\partial^i) < r_V + r_U$, we must have $\operatorname{ord}(\partial^i T - \operatorname{rquo}(\partial^i S, S')T') < r_U$ for all such i. This implies that the image of the Sylvester matrix contains all unit vectors in $K^{r_V + r_U}$, and thus consists of the full space. The kernel is therefore just $\{0\}$, and this in turn implies that the resultant is nonzero. We have thus shown that $\operatorname{gcrd}(U, V) = 1$ if and only if $\operatorname{res}(U, V) \neq 0$.

In the general case, suppose the greatest common right divisor of U and V has order r. Then in the linear system above we have $g_r = 1$ and $g_{r+1} = \cdots = g_{r_U+r_V-1} = 0$, and if we cut away the rows corresponding to $g_0, \ldots, g_{r-1}$, we obtain the following linear system for the coefficients of S and T:



Every solution vector $(s_0, \ldots, t_0, \ldots) \in K^{r_u + r_v}$ of this system gives rise to operators $S, T \in K[\partial]$ such that $SU + TV = \partial^r + \cdots$. The right hand side must in fact be the greatest common right divisor of U and V, because the greatest common right divisor of U and V must be a right divisor of the left hand side, hence also of the right side, and since both the gcrd and the right hand side have order r, they must be equal.

By part 3 of Theorem 4.21 we also know that we may assume $s_{r_V - i} = 0$ for $i = 1, \ldots, r$ and $t_{r_U - i} = 0$ for $i = 1, \ldots, r$, so we can remove these variables from the linear system and delete the corresponding columns from the Sylvester matrix. Since $[\partial^k]\partial^i U = 0$ for $k > i + r_U$ and $[\partial^k]\partial^i V = 0$ for $k > i + r_V$, the Sylvester matrix contains zeros in the areas indicated by the unshaded triangular regions in the figure above. Removing the $2r$ unnecessary columns will therefore leave us with a matrix that has at least r rows that only contain zeros, and we may drop these as well. The situation then looks as follows:



As a result of this discussion, we get an alternative algorithm for computing $\operatorname{gcrd}(U, V)$: solve the above linear system in turn for $r = 0, 1, 2, \ldots$. The first r for which the system has a solution gives us the cofactors S, T from which we can get the final result via $\operatorname{gcrd}(U, V) = SU + TV$. This algorithm has the nice feature that it gives us access to a bound on the size of the coefficients that may appear in the gcrd.

Theorem 4.23 *Suppose that $K = C(x)$ and that $\sigma, \delta \colon K \to K$ map polynomials to polynomials and do not increase degrees, i.e.,* $\deg(\sigma(p)), \deg(\delta(p)) \le \deg(p)$ *for all $p \in C[x]$. Let $U, V \in C[x][\partial] \subseteq K[\partial]$ be such that $U, V \neq 0$ and* $\operatorname{lc}(V)U \neq \operatorname{lc}(U)V$. *Let $r_U = \operatorname{ord}(U)$, $r_V = \operatorname{ord}(V)$, and let $d_U, d_V \in \mathbb{N}$ be such that all coefficients of U have degree at most d_U and all coefficients of V have degree at most d_V. Let $G = \operatorname{gcrd}(U, V) \in K[\partial]$ and $r = \operatorname{ord}(G)$. Then the coefficients of G are elements of $C(x)$ whose numerators and denominators are polynomials of degree at most $(r_V - r)d_U + (r_U - r)d_V$.* □

Proof Continuing the preceding discussion, we find that the combined coefficient vector

$$(s_0, \ldots, s_{r_V - r - 1}, t_0, \ldots, t_{r_U - r - 1})$$

of $S, T \in K[\partial]$ such that $\operatorname{gcrd}(U, V) = SU + TV$ is a solution of an inhomogeneous linear system obtained from the Sylvester matrix by deleting $2r$ rows and $2r$ columns. Because of the assumptions on σ and δ, we have $\deg([\partial^k]\partial^i U) \le d_U$ and $\deg([\partial^k]\partial^i V) \le d_V$ for all i and k, so that the matrix has $r_V - r$ columns with entries of degree at most d_U and $r_U - r$ columns with entries of degree at most d_V. By Cramer's rule, the denominator of the coefficients of S and T is the determinant of this matrix, i.e., a polynomial of degree at most $(r_V - r)d_U + (r_U - r)d_V$, the numerators of the coefficients of S are polynomials of degree at most $(r_V - r)d_U + (r_U - r)d_V - d_U$, and the numerators of the coefficients of T are polynomials of degree at most $(r_V - r)d_U + (r_U - r)d_V - d_V$. The announced bound for $G = SU + TV$ follows. ■

In the setting of this theorem, a greatest common right divisor can be computed in polynomial time, because it suffices to solve at most r_V linear systems of size at most $(r_U + r_V) \times (r_U + r_V)$ with polynomial entries of degree at most d_U, d_V. A naive implementation of Algorithm 4.20 will be slower, because the coefficients of G, S, T can grow dramatically during the execution of the loop, even though Theorem 4.23 guarantees that the final result will be of reasonable size. What lets the size drop in the end is the multiplication with $\mathrm{lc}(G)^{-1}$ from the left, and for an implementation of Algorithm 4.20 we reiterate the advice to introduce such a normalization step in each iteration of the loop. In the case $K = C(x)$, an even more careful implementation will avoid working with rational functions and ensure that G belongs to $C[x][\partial]$ at all times, and that the coefficients of G are coprime (assuming, as usual, that they are written to the left of the powers of ∂).

The greatest common right divisor is useful for showing that every left ideal of $K[\partial]$ is generated by a single element. It is also useful for describing the intersection of two solution spaces. The details are as follows.

Theorem 4.24 *Let F be a $K[\partial]$-module and let $A, B \in K[\partial]$. Then*

1. $V(A) \cap V(B) = V(\mathrm{gcrd}(A, B))$.
2. $\langle A, B\rangle = \langle \mathrm{gcrd}(A, B)\rangle$. □

Proof

1. "$\subseteq$": If $f \in V(A)\cap V(B)$, then $A\cdot f = B\cdot f = 0$, and then $(SA+TB)\cdot f = 0$ for every $S, T \in K[\partial]$. Taking S, T appropriately, we find $\mathrm{gcrd}(A, B) \cdot f = 0$, so $f \in V(\mathrm{gcrd}(A, B))$.
   "$\supseteq$": Writing $G = \mathrm{gcrd}(A, B)$, we have $A = \tilde{A}G$ and $B = \tilde{B}G$ for certain $\tilde{A}, \tilde{B} \in K[\partial]$, so if $f \in V(\mathrm{gcrd}(A, B))$, then $G \cdot f = 0$ implies $A \cdot f = (\tilde{A}G) \cdot f = \tilde{A} \cdot (G \cdot f) = \tilde{A} \cdot 0 = 0$ and similarly, $B \cdot f = (\tilde{B}G) \cdot f = 0$, so $f \in V(A) \cap V(B)$.
2. "$\subseteq$": With $G = \mathrm{gcrd}(A, B)$, we have $A = \tilde{A}G$ and $B = \tilde{B}G$ for certain $\tilde{A}, \tilde{B} \in K[\partial]$. Every $P \in \langle A, B\rangle$ can be written as $P = UA + VB$ for certain $U, V \in K[\partial]$, and $P = UA + VB = (U\tilde{A} + V\tilde{B})G$ shows $P \in \langle G\rangle$.
   "$\supseteq$": With $G = \mathrm{gcrd}(A, B)$ and $S, T \in K[\partial]$ such that $G = SA + TV$, every element $P \in \langle G\rangle$, say $P = \tilde{P}G$ for some $\tilde{P} \in K[\partial]$, can be written as $P = \tilde{P}SA + \tilde{P}SB$ and therefore belongs to $\langle A, B\rangle$. ■

Let us now turn from the greatest common right divisor to the least common left multiple. In the commutative case, the greatest common divisor and the least common left multiple are related through the formula $\mathrm{lc}(p)\,\mathrm{lc}(q)\,\mathrm{gcd}(p, q)\,\mathrm{lcm}(p, q) = pq$ (Exercise 11), which holds for all $p, q \in C[x]$ and allows us to compute either one of $\mathrm{gcd}(p, q), \mathrm{lcm}(p, q)$ if we know how to compute the other. Unfortunately, the formula does not hold in the general Ore setting. For example, for $U = xD - 1$ and $V = D + 1$, we have $UV = xD^2 + (x - 1)D - 1$, $\mathrm{gcrd}(U, V) = 1$, and $\mathrm{lclm}(U, V) = (x + 1)D^2 + xD - 1$. Also, $VU = xD^2 + xD - 1$ does not match.

Before we discuss the computation of least common left multiples, observe that the least common left multiple of $U, V \in K[\partial]$ in the sense of Definition 4.19 is at the same time a common left multiple of minimal order. For if $P \in K[\partial] \setminus \{0\}$ is a common left multiple of U, V of minimal order and $P' \in K[\partial]$ is another common left multiple of U, V, then $\operatorname{rrem}(P', P) = P'P - \operatorname{rquo}(P', P)P$ is also a common left multiple of U and V, and since $\operatorname{ord}(\operatorname{rrem}(P', P)) < \operatorname{ord}(P)$ and $\operatorname{ord}(P)$ is minimal, we must have $\operatorname{rrem}(P', P) = 0$, which is exactly the condition for P to be a right divisor of P. With this knowledge, we can prove the following theorem, which contains some counterparts of the previous theorem and reveals that we have met the least common left multiple already in the previous section.

Theorem 4.25 *Let F be a $K[\partial]$-module and let $A, B \in K[\partial]$. Then*

1. $V(A) + V(B) \subseteq V(\operatorname{lclm}(A, B))$.
2. $\langle A\rangle \cap \langle B\rangle = \langle \operatorname{lclm}(A, B)\rangle$.
3. $\operatorname{lclm}(A, B) = A \oplus B$. □

Proof

1. Writing $m = \operatorname{lclm}(u, v)$, we have $m = \tilde{u}u = \tilde{v}v$ for certain $\tilde{u}, \tilde{v} \in K[\partial]$, so if $f \in V(u) + V(v)$, say $f = f_u + f_v$ for some $f_u \in V(u)$ and some $f_v \in V(v)$, then $m \cdot f = m \cdot (f_u + f_v) = (m \cdot f_u) + (m \cdot f_v) = (\tilde{u}u \cdot f_u) + (\tilde{v}v \cdot f_v) = 0$, so $f \in V(m)$.
2. "$\subseteq$": If $P \in \langle A\rangle \cap \langle B\rangle$, then $P = \tilde{A}A = \tilde{B}B$ for certain $\tilde{A}, \tilde{B} \in K[\partial]$, so P is a common left multiple of A and B, and therefore a left multiple of $\operatorname{lclm}(A, B)$, and therefore an element of $\langle \operatorname{lclm}(A, B)\rangle$.
   "$\supseteq$": If $M = \operatorname{lclm}(A, B)$, then $M = \tilde{A}A = \tilde{B}B$ for certain $\tilde{A}, \tilde{B} \in K[\partial]$, and if $P \in \langle \operatorname{lclm}(A, B)\rangle$, then $P = \tilde{M}M$ for some $\tilde{M} \in K[\partial]$, and $P = \tilde{M}\tilde{A}A = \tilde{M}\tilde{B}B$ shows that $P \in \langle A\rangle \cap \langle B\rangle$.
3. Recall that $A \oplus B$ was defined as the monic minimal annihilating operator of $([1], [1]) \in K[\partial]/\langle A\rangle \times K[\partial]/\langle B\rangle$. With the definition of the action of $K[\partial]$ on this module, we have $M \cdot ([1], [1]) = ([M], [M]) = ([0], [0])$ if and only if $M \in \langle A\rangle \cap \langle B\rangle$. It follows from the previous part that $\langle \operatorname{lclm}(A, B)\rangle$ is the annihilator of $([1], [1])$. Since $\operatorname{lclm}(A, B)$ is the unique monic element of minimal order in this ideal, it must be equal to $A \oplus B$. ■

Observe that only one inclusion is claimed in part 1. The other inclusion is false in general. Counterexamples can be constructed from elements of $K[\partial]$ whose solution space in F does not have the largest possible dimension.

Example 4.26 Consider the action of $C(x)[D]$ on $F = C(x)$ and let $A = xD^2 + D$ and $B = x(x + 1)D^2 + D$. We then have $\operatorname{lclm}(A, B) = xD^3 + 2D^2$, and it can be checked that both $V(A)$ and $V(B)$ are C-vector spaces generated by 1, so $V(A) + V(B) = V(A) = V(B)$. However, $V(\operatorname{lclm}(A, B))$ contains the additional polynomial $x \notin V(A) + V(B)$.

It becomes more clear what is going on if we replace F by a larger differential field. In $F = C(x, \log(x))$, the vector space $V(A)$ is generated by 1 and $\log(x)$, and the vector space $V(B)$ is generated by 1 and $x + \log(x)$. We see that in this case, $V(A) + V(B)$ contains the missing solution x of $\operatorname{lclm}(A, B)$. □

Part 3 of Theorem 4.25 motivates the following algorithm for computing the least common left multiple of any two elements of $K[\partial]$.

Algorithm 4.27 *(Least common left multiple)*
Input: $U, V \in K[\partial]$.
Output: $\operatorname{lclm}(U, V) \in K[\partial]$.

1 *if* $U = 0$ *or* $V = 0$ *then*
2   *Return* 0.
3 *Set* $U_0 = V_0 = 1 \in K[\partial]$.
4 *for* $r = 1, 2, \ldots,$ *do*
5   *Compute* $U_r = \operatorname{rrem}(\partial U_{r-1}, U) \in K[\partial]$.
6   *Compute* $V_r = \operatorname{rrem}(\partial V_{r-1}, V) \in K[\partial]$.
7   *Check whether there exists* $(p_0, \ldots, p_r) \in K^{r+1} \setminus \{0\}$ *with*

$$p_0U_0 + \cdots + p_rU_r = p_0V_0 + \cdots + p_rV_r = 0.$$

8   *if yes then*
9   *Return* $\frac{p_0}{p_r} + \frac{p_1}{p_r}\partial + \cdots + \frac{p_{r-1}}{p_r}\partial^{r-1} + \partial^r$.

Theorem 4.28 *Algorithm 4.27 is correct and terminates. In particular, we have*

$$\operatorname{ord}(\operatorname{lclm}(U, V)) \leq \operatorname{ord}(U) + \operatorname{ord}(V)$$

for all $U, V \in K[\partial] \setminus \{0\}$. □

Proof First note that for all $i \in \mathbb{N}$ we have $U_i = \operatorname{rrem}(\partial^i, U)$ and $V_i = \operatorname{rrem}(\partial^i, V)$, so that line 7 ensures that

$$\operatorname{rrem}(p_0 + p_1\partial + \cdots + p_r\partial^r, U) = \operatorname{rrem}(p_0 + p_1\partial + \cdots + p_r\partial^r, V) = 0,$$

which means that $P = p_0 + p_1\partial + \cdots + p_r\partial^r$ is a common left multiple of U and V. If we find a nonzero coefficient vector $(p_0, \ldots, p_r)$ in this step, we must have $p_r \neq 0$, for otherwise we would have found the solution already in an earlier iteration. It is therefore safe to divide by p_r (from the left) and to return $p_r^{-1}P$ as the correct result.

For the termination, observe that every U_i is a K-linear combination of the powers $1, \partial, \ldots, \partial^{\operatorname{ord}(U)-1}$ and that each V_i is a K-linear combination of $1, \partial, \ldots, \partial^{\operatorname{ord}(V)-1}$. Therefore, the coefficient comparison with respect to powers of ∂ done in line 7 leads to a linear system with $\operatorname{ord}(U) + \operatorname{ord}(V)$ equations and $r + 1$ equations, which must have a solution as soon as $r > \operatorname{ord}(U) + \operatorname{ord}(V)$. This proves termination as well as the claimed bound on the order of the output. ■

Example 4.29

1. In $C(x)[D]$, consider $U = (2x + 3)xD^2 + 2(4x^2 + 3x - 3)D + 2(4x^2 - 3)$, $V = (x+1)(x-1)D^2 + 2(2x^2 - x - 2)D + 2(2x^2 - 2x - 1)$. With $U_0 = V_0 = 1$ and $U_1 = V_1 = D$ we obviously have no nontrivial solution yet. In the next step, we get

$$U_2 = \operatorname{rrem}(D^2, U) = \frac{2(4x^2+3x-3)}{x(2x+3)}D - \frac{2(4x^2-3)}{x(2x+3)},$$
$$V_2 = \operatorname{rrem}(D^2, V) = \frac{2(2x^2-x-2)}{(x+1)(x-1)}D - \frac{2(2x^2-2x-1)}{(x+1)(x-1)},$$

and there could be $p_0, p_1, p_2 \in K$ such that $p_0U_0 + p_1U_1 + p_2U_2 = p_0V_0 + p_1V_1 + p_2V_2 = 0$. Coefficient comparison leads to the linear system

$$\begin{pmatrix} 1 & 0 & -\frac{2(4x^2-3)}{x(2x+3)} \\ 0 & 1 & \frac{2(4x^2+3x-3)}{x(2x+3)} \\ 1 & 0 & -\frac{2(2x^2-2x-1)}{(x+1)(x-1)} \\ 0 & 1 & \frac{2(2x^2-x-2)}{(x+1)(x-1)} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = 0,$$

whose only solution is zero. We continue with

$$U_3 = \frac{6(x-1)(4x^2-4x-1)}{x^2(2x+3)}D + \frac{2(16x^3-12x^2-12x+3)}{x^2(2x+3)},$$
$$V_3 = \frac{12(x^2-x-1)}{(x+1)(x-1)}D + \frac{4(4x^2-6x-1)}{(x+1)(x-1)},$$

but will still not find a solution. In the next step, we have

$$U_4 = \frac{16(4x^3-3x^2-6x+3)}{x^2(2x+3)}D - \frac{48(2x-1)(x^2-x-1)}{x^2(2x+3)},$$
$$V_4 = \frac{16(2x+1)(x-2)}{(x+1)(x-1)}D - \frac{48x(x-2)}{(x+1)(x-1)},$$

and the corresponding linear system

$$\begin{pmatrix} 1 & 0 & -\frac{2(4x^2-3)}{x(2x+3)} & \frac{2(16x^3-12x^2-12x+3)}{x^2(2x+3)} & -\frac{48(2x-1)(x^2-x-1)}{x^2(2x+3)} \\ 0 & 1 & \frac{2(4x^2+3x-3)}{x(2x+3)} & \frac{6(x-1)(4x^2-4x-1)}{x^2(2x+3)} & \frac{16(4x^3-3x^2-6x+3)}{x^2(2x+3)} \\ 1 & 0 & -\frac{2(2x^2-2x-1)}{(x+1)(x-1)} & \frac{4(4x^2-6x-1)}{(x+1)(x-1)} & -\frac{48x(x-2)}{(x+1)(x-1)} \\ 0 & 1 & \frac{2(2x^2-x-2)}{(x+1)(x-1)} & \frac{12(x^2-x-1)}{(x+1)(x-1)} & \frac{16(2x+1)(x-2)}{(x+1)(x-1)} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} = 0$$

must have a nonzero solution because it has more variables than equations. A basis vector of the solution space translates into the operator

$$\operatorname{lclm}(U, V) = D^4 + 8D^3 + 24D^2 + 32D + 16.$$

This is really a common left multiple of U and V because we have

$$\operatorname{lclm}(U, V) = \Big(\frac{1}{x(2x+3)}D^2 + \frac{2(4x+5)}{x(2x+3)^2}D + \frac{8(x+1)}{x(2x+3)^2}\Big)U$$
$$= \Big(\frac{1}{(x+1)(x-1)}D^2 + \frac{2(2x^2-x-2)}{(x+1)^2(x-1)^2}D + \frac{4(x^2-x-1)}{(x+1)^2(x-1)^2}\Big)V.$$

2. In $C(x)[S]$, consider $U = (x+2)(2x-1)S^2 - 8(x^2+3x-1)S + 4(x+4)(2x+1)$ and $V = (x+4)(x+3)S^2 - 2(x+5)(2x+5)S + 4(x+4)(x+5)$. An analogous computation as above yields

$$\operatorname{lclm}(U, V) = S^3 - \frac{2(3x+10)}{x+3}S^2 + \frac{4(3x+11)}{x+3}S - \frac{8(x+4)}{x+3},$$

and this is really a common left multiple because it can be written as

$$\operatorname{lclm}(U, V) = \Big(\frac{1}{(2x+1)(x+3)}S - \frac{2}{(2x+1)(x+3)}\Big)U$$
$$= \Big(\frac{1}{(x+5)(x+3)}S - \frac{2}{(x+5)(x+3)}\Big)V.$$

□

Again, we observe a phenomenon that cannot happen in the commutative case: the coefficients of the least common left multiple are smaller than those of the input. This does not happen generically, but as the example shows, it can happen. What happens generically though is that higher order common left multiples may have lower degree than the least common left multiple.

Theorem 4.30 *Suppose that $K = C(x)$ and that $\sigma, \delta\colon K \to K$ map polynomials to polynomials and do not increase degrees, i.e.,* $\deg(\sigma(p)), \deg(\delta(p)) \le \deg(p)$ *for all $p \in C[x]$. Let $U, V \in C[x][\partial] \subseteq K[\partial]$, $r_U = \operatorname{ord}(U)$, $r_V = \operatorname{ord}(V)$, and let $d_U, d_V \in \mathbb{N}$ be such that all coefficients of U have degree at most d_U and all coefficients of V have degree at most d_V.*

1. *Let $P = \operatorname{lclm}(U, V) \in K[\partial]$ and $r = \operatorname{ord}(P)$. Then the coefficients of P are elements of $C(x)$ whose numerators and denominators are polynomials of degree at most*

$$(r + 1 - r_V)d_U + (r + 1 - r_U)d_V.$$

2. *For every $r \ge r_U + r_V$ and every*

$$d > d_U + d_V - 1 + \frac{r_V d_U + r_U d_V}{r - r_U - r_V + 1}$$

there exists a common left multiple of U and V of order r with polynomial coefficients of degree at most d. □

Proof

1. If $S, T \in K[\partial]$ are such that $P = SU = TV$, then $\operatorname{ord}(S) = r - r_U$ and $\operatorname{ord}(T) = r - r_V$. Consider an ansatz

$$(s_0 + s_1\partial + \cdots + s_{r-r_U}\partial^{r-r_U})U - (t_0 + t_1\partial + \cdots + t_{r-r_V}\partial^{r-r_V})V = 0$$

with undetermined coefficients $s_0, \ldots, s_{r-r_U}$ and $t_0, \ldots, t_{r-r_V}$. Equating coefficients of ∂^i to zero, for $i = 0, \ldots, r$, leads to a linear system with $(r - r_U + 1) + (r - r_V + 1)$ variables and $r + 1$ equations. By assumption on σ and δ, the corresponding matrix has $r - r_U + 1$ columns with entries of degree at most d_U and $r - r_V + 1$ columns with entries of degree at most d_V. Because of the uniqueness of $\operatorname{lclm}(U, V)$, the linear system has a solution space in $C(x)^{2r+2-r_U-r_V}$ of dimension 1, so the corresponding matrix has rank $2r + 1 - r_U - r_V$. By Theorem 1.29, the solution space is generated by a vector $(s_0, \ldots, s_{r-r_U}, t_0, \ldots, t_{r-r_V}) \in C[x]^{2r+2-r_U-r_V}$ with

$$\deg(s_i) \le (r + 1 - r_V)d_U + (r + 1 - r_U)d_V - d_U \quad \text{and}$$
$$\deg(t_j) \le (r + 1 - r_V)d_U + (r + 1 - r_U)d_V - d_V$$

for all $i = 0, \ldots, r - r_U$ and $j = 0, \ldots, r - r_V$. The announced degree bound for $P = SU = TV$ follows.

2. Let $r \ge r_U + r_V$ and $d > d_U + d_V - 1 + \frac{r_V d_U + r_U d_V}{r - r_U - r_V + 1}$ and make an ansatz

$$S = \sum_{i=0}^{r-r_U} \sum_{j=0}^{d-d_U} s_{i,j} x^j \partial^i \qquad T = \sum_{i=0}^{r-r_V} \sum_{j=0}^{d-d_V} t_{i,j} x^j \partial^i$$

with undetermined coefficients $s_{i,j}, t_{i,j} \in C$. We show that these coefficients can be instantiated such that $SU = TV$. Indeed, equating the coefficients of $SU - TV$ with respect to $x^j\partial^i$ to zero gives a C-linear system with $(r - r_U + 1)(d - d_U + 1) + (r - r_V + 1)(d - d_V + 1)$ variables and no more than $(r + 1)(d + 1)$ equations. Because of the assumption on d, we have

$$\begin{aligned}
&(r - r_U + 1)(d - d_U + 1) + (r - r_V + 1)(d - d_V + 1) - (r + 1)(d + 1)\\
&= (r + 1 - r_U - r_V)(d + 1 - d_U - d_V) - r_V d_U - r_U d_V\\
&> (r + 1 - r_U - r_V)\Big(d_U + d_V - 1 + \frac{r_V d_U + r_U d_V}{r - r_U - r_V + 1} + 1 - d_U - d_V\Big)\\
&\qquad - r_V d_U - r_U d_V\\
&= 0
\end{aligned}$$

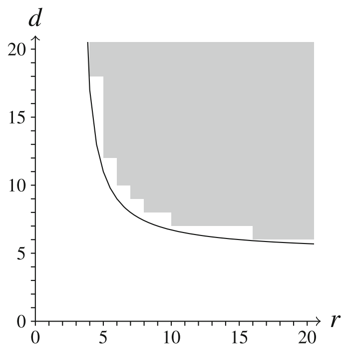
and therefore more variables than equations. The nontrivial solution gives rise to a common left multiple SU whose order may still be less than r, because some of the coefficients $s_{i,j}$ of the nonzero solution may be zero. But since also $\partial^i SU$ is a common left multiple for every choice of i, we can get a left multiple of order exactly r with coefficients of degree at most d. ■

Example 4.31 Consider the operators

$$U = (2x^3 + 2x^2 + 8)D^2 + (7x^2 + 5x + 3)D + (3x^3 + x^2 + x + 7),$$

$$V = (9x^3 + 8x^2 + 6x + 3)D^2 + (3x^3 + 2x^2 + 7x + 5)D + (4x^3 + x + 9).$$

In the following figure, the gray region marks all the points (r, d) for which there exists a common left multiple of U and V of order r and degree d. By the theorem above, all points $(r, d) \in \mathbb{N}^2$ satisfying $d \geq 5 + \frac{12}{r-3}$ belong to this gray region. As the white space between the curve and the gray region contains no points with integer coordinates, the bounds provided by the theorem are sharp in this example.



□

Part 2 of Theorem 4.30 allows us to get common left multiples of smaller degree if we allow for larger orders. If we allow a very large order, we can get the degree down to $d_U + d_V$. In general, there will not exist a common left multiple of lower degree. Just consider two differential operators $U, V \in C[x][D]$ whose leading coefficients are squarefree coprime polynomials of degree d_U and d_V, respectively, with roots that are non-apparent singularities in the sense of Definition 3.17. Since every solution of U or V must also be a solution of any common left multiple of U and V, any such left multiple must have a leading coefficient that is a multiple of $\operatorname{lcm}(\operatorname{lc}(U), \operatorname{lc}(V))$, and if $\operatorname{lc}(U)$ and $\operatorname{lc}(V)$ are coprime as elements of $C[x]$, the degree of $\operatorname{lcm}(\operatorname{lc}(U), \operatorname{lc}(V)) = \operatorname{lc}(U)\operatorname{lc}(V)$ is $d_U + d_V$.

If there are apparent singularities, the degrees of the left multiples may be smaller than the bound of Theorem 4.30. In fact, we can use left multiples to lift the discussion of apparent singularities of Sect. 3.2 to arbitrary Ore algebras. We do not even need to refer to solutions of an operator.

Definition 4.32 Let $P \in C[x][\partial]$, $r = \operatorname{ord}(P)$, and let $p \in C[x]$ be a factor of $\operatorname{lc}(P)$. Let $n \in \mathbb{N}$. We say that p is *removable* from P at cost n if there exists an operator $Q \in C(x)[\partial]$ such that $QP \in C[x][\partial]$ and $\operatorname{lc}(QP) \mid \sigma^n(\operatorname{lc}(P)/p)$. In this case, we say that Q is a *p-removing* operator for P. □

For example, if $P = xD - 5 \in C[x][D]$, the factor $p = x$ is removable at cost $n = 5$ because for $Q = \frac{1}{x}D^5$ we have $QP = D^6$. This is in line with the examples we discussed in Sect. 3.2, but removability as defined above is not restricted to the differential case. For example, if $P = xS - (x+3) \in C[x][S]$, the factor $p = x$ is removable at cost $n = 3$, because for $Q = \frac{1}{x+3}(S-1)^3$ we have $QP = S^4 - 4S^3 + 6S^2 - 4S + 1$. One application of removing factors is that with a bit of luck it may allow us to show that a D-finite sequence has only integer terms.

Example 4.33

1. Consider the D-finite sequence $(a_n)_{n=0}^\infty$ defined by $a_0 = 2$, $a_1 = 3$, $a_3 = 14$, and

$$(n-1)a_{n+2} = (n^2 + 3n - 2)a_{n+1} - 2n(n+1)a_n \qquad (n \in \mathbb{N}).$$

   Computing the nth term of the sequence with this recurrence requires a division by $n-3$, and there is no obvious reason why this division should always produce integers. But in fact it does, because $x+1$ is removable for the operator $P = (x-1)S^2 - (x^2+3x-2)S + 2x(x+1) \in C[x][S]$. More precisely, we have

$$\tfrac{1}{x}(S-2)P = S^3 - (x+7)S^2 + 4(x+3)S - 4(x+1),$$

   so the sequence $(a_n)_{n=0}^\infty$ also satisfies the recurrence

$$a_{n+3} = (n+7)a_{n+2} - 4(n+3)a_{n+1} - 4(n+1)a_n,$$

   from which it can easily be seen that $a_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$.
2. An operator whose leading coefficient has non-removable factors may nevertheless have integer sequence solutions. For example $P = (x+2)S - (4x+2) \in C[x][S]$ is an annihilating operator for the sequence $(C_n)_{n=0}^\infty$ of Catalan numbers, and while we clearly have $C_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$, the factor $x+2$ is not removable. □

If $p \in C[x]$ is irreducible and $k \in \mathbb{N}$, then according to Exercise 18 a p^k-removing operator can be assumed to be of the form

$$Q = \frac{1}{\sigma^n(p)^{e_n}}\partial^n + \frac{q_{n-1}}{\sigma^n(p)^{e_{n-1}}}\partial^{n-1} + \cdots + \frac{q_0}{\sigma^n(p)^{e_0}}$$

for some $e_0, \ldots, e_n \in \mathbb{N}$ and some $q_0, \ldots, q_{n-1} \in C[x]$ with $\deg(q_i) < e_i \deg(p)$ ($i = 0, \ldots, n-1$). If someone gives us suitable n and $e_0, \ldots, e_n$, we can find $q_0, \ldots, q_{n-1}$ by making an ansatz $q_i = \sum_{j=0}^{e_i \deg(p)-1} q_{i,j}x^j$ with undetermined coefficients $q_{i,j}$, computing QP, and forcing its coefficients to be polynomials. A priori, the coefficients of QP are rational functions whose numerators can be written as a linear combination of the unknown coefficients, and they become polynomials whenever the numerators are multiples of the denominators. We can enforce this by computing the remainders of all numerators with respect to the corresponding denominators and equate their coefficients to zero. This gives an inhomogeneous linear system for the unknowns $q_{i,j}$, which may or may not have a solution. If it has a solution and we instantiate $q_{i,j}$ accordingly, then Q is a p^k-removing operator for P.

The choice of n and $e_0, \dots, e_n$ depends on the particular Ore algebra at hand. For the differential case, desingularization is covered in Sect. 3.3. For other algebras, bounds on n and $e_0, \dots, e_n$ can be found in the literature.

There is another, more pragmatic, way to remove removable factors by computing a least common left multiple. In the proof of Theorem 4.30, we used an ansatz

$$(s_0 + s_1\partial + \cdots + s_{r_V}\partial^{r_V})U = (t_0 + t_1\partial + \cdots + t_{r_U}\partial^{r_U})V$$

and compared coefficients to obtain a linear system of equations whose solution vectors gave rise to the coefficients of operators S, T that we can multiply from the left to U, V, respectively, to obtain a common left multiple of U and V. We have some freedom to modify this ansatz. Suppose, for example, that $\mathrm{lc}(U)$ contains an irreducible factor $p \in C[x]$ which is removable at cost n, and that $Q \in C(x)[\partial]$ is a p-removing operator of order n. Consider the alternative ansatz

$$(s_0 + s_1\partial + \cdots + s_{n-1}\partial^{n-1} + s_n Q)U = (t_0 + t_1\partial + \cdots + t_{r_U}\partial^{r_U})V.$$

When $(s_0, \dots, s_n, t_0, \dots, t_{r_U}) \in C[x]^{n+r_U+2}$ is a nonzero solution vector of the resulting linear system, then $(s_0 + s_1\partial + \cdots + s_{n-1}\partial^{n-1} + s_n Q)U$ is a left multiple of U whose leading coefficient is $s_n\,\mathrm{lc}(QU)$, which is not a multiple of $\sigma^n(p)$ unless $\sigma^n(p)$ happens to be a factor of s_n. It can be shown that only for very few choices of V will it happen that $\sigma^n(p) \mid s_n$, so if we randomly choose an operator $V \in C[x][\partial]$ of order n, we can expect that left-multiplying $\mathrm{lclm}(U, V) \in C(x)[\partial]$ with the common denominator of its coefficients yields a left-multiple of U which lives in $C[x][\partial]$ and whose leading coefficient does not contain $\sigma^n(p)$ as a factor.

Note that although we assumed the knowledge about a p-removing operator Q in the discussion above, we do not actually need to know Q for computing $\mathrm{lclm}(U, V)$.

Note also that taking the least common left multiple of U with some other operator V is not only likely to remove removable factors, but it is also likely to introduce new factors. In general, the factor s_n of the new leading coefficient is not just a constant. In order to get a left-multiple of U with a smaller leading coefficient, we compute $g = \gcd(\mathrm{lc}(P), \sigma^n(\mathrm{lc}(U)))$ and $s, t \in C[x]$ with $g = s\,\mathrm{lc}(P) + t\sigma^n(\mathrm{lc}(U))$. Then $sP + t\partial^n U$ is a left-multiple of U whose leading coefficient g contains neither $\sigma^n(p)$ nor the factors that have been introduced by the lclm-computation.

Exercises

1*. Let $A, B, C \in K[\partial]$, $C \neq 0$. Prove or disprove:

a. $\operatorname{rrem}(A, C) + \operatorname{rrem}(B, C) = \operatorname{rrem}(A + B, C)$.

b. $\operatorname{rrem}(A \operatorname{rrem}(B, C), C) = \operatorname{rrem}(AB, C)$.

c. $\operatorname{rrem}(\operatorname{rrem}(A, C)B, C) = \operatorname{rrem}(AB, C)$.

2. Show that for any $U, V \in K[\partial]$, there can be at most one greatest common right divisor and at most one least common left multiple.

3. Show that $\operatorname{gcrd}(U, \operatorname{gcrd}(V, W)) = \operatorname{gcrd}(\operatorname{gcrd}(U, V), W)$ for all $U, V, W \in K[\partial]$.

4. Compute $\operatorname{gcrd}(U, V)$ for $U = (x + 1)\partial^2 + (x^2 + 2x - 1)\partial - x^2(x + 1)$, $V = (x+1)\partial^2 + (3x+1)\partial - 2x(x+1) \in C(x)[\partial]$ with $\sigma\colon C(x) \to C(x)$ defined by $\sigma(p(x)) = p(\frac{1-x}{1+x})$ for $p(x) \in C(x)$ and $\delta = 0$.

5. Compute S, T such that $\operatorname{gcrd}(U, V) = SU + TV$ for the two pairs of operators U, V considered in Example 4.22.

6*. Show part 4 of Theorem 4.21. *Hint:* First consider the case where U, V are coprime.

7. Let $U, V \in K[\partial] \setminus \{0\}$ and $G = \operatorname{gcrd}(U, V)$. Show that $S, T \in K[\partial]$ with $G = SU + TV$ and $\operatorname{ord}(S) < \operatorname{ord}(V) - \operatorname{ord}(G)$ and $\operatorname{ord}(T) < \operatorname{ord}(U) - \operatorname{ord}(G)$ do not exist if $U = cV$ for some $c \in K \setminus \{0\}$.

8*. Let $\sigma, \delta\colon C[x] \to C[x]$ be such that $\deg(\sigma(p)), \deg(\delta(p)) < \deg(p)$ for all $p \in C[x]$. Suppose that the application of σ or δ to a given polynomial $p \in C[x]$ of degree at most d costs $O^\sim(d)$ operations in C. Let $r, d \in N$, and let $U, V \in C[x][\partial]$ with $\operatorname{ord}(V) < \operatorname{ord}(U) \leq r$ and with coefficients of degree at most d. Show that $\operatorname{gcrd}(U, V) \in C(x)[\partial]$ can be computed using $O^\sim(r^\omega d)$ operations in C.

9. Find all $\alpha \in C$ for which $U = S^2 + (1 + 2x - x^2)S - x^2(x - \alpha)$ and $V = S^2 + \alpha S - x(x + \alpha - 1)$ have a nontrivial greatest common right divisor.

10*. A consequence of Theorem 4.24 is that $K[\partial]$ is a principle left ideal domain, i.e., every left ideal of $K[\partial]$ is generated by a single element. In contrast, show that $C[x][\partial]$ is in general not a principle left ideal domain.

11*. Show that $\operatorname{lc}(p)\operatorname{lc}(q)\gcd(p, q)\operatorname{lcm}(p, q) = pq$ for all $p, q \in C[x]$. Where do you need commutativity?

12*. Let $a, b \in C(x) \setminus \{0\}$ and consider an algebraic function y with minimal polynomial $y^2 + ay + b$. Let $L \in C(x)[D]$ be the monic minimal order annihilating operator of y (cf. Theorem 3.29). Show that L is a least common left multiple of two first order operators.

13*. Show that we have $\operatorname{ord}(U) + \operatorname{ord}(V) = \operatorname{ord}(\operatorname{gcrd}(U, V)) + \operatorname{ord}(\operatorname{lclm}(U, V))$ for all $U, V \in K[\partial] \setminus \{0\}$.

14*. When the extended Euclidean algorithm terminates, the components of (G, S, T, G', S', T') are such that $G = \operatorname{gcrd}(U, V) = SU + TV$ and $G' = 0$. Show that furthermore, $\operatorname{lclm}(U, V) = aS'U = bT'V$ for certain nonzero $a, b \in K$.

Hint: Consider the $K[\partial]$-submodule of $K[\partial]^3$ generated by $(U, 1, 0)$ and $(V, 0, 1)$.

15. Compute $\operatorname{lclm}(U, V)$ for U, V from Exercise 4, for the following settings:

a. $\sigma(p(x)) = p(\frac{x-1}{x+1})$ for all $p \in C(x)$, and $\delta = 0$;

b. $\sigma = \mathrm{id}$ and $\delta = 0$;

c. $\sigma = \mathrm{id}$ and $\delta(p(x)) = \frac{x-1}{x+1}p'(x)$ for all $p \in C(x)$.

16. Find $A, B \in C(x)[S]$ and a $C(x)[S]$-module F such that $V(A) + V(B) \subsetneq V(\operatorname{lclm}(A, B))$ in F (cf. Example 4.26).

17.** Let $\sigma, \delta\colon C[x] \to C[x]$ be as in Exercise 8. Let $r \in N, d \in \mathbb{N}$ and $U, V \in C[x][\partial]$ with $\operatorname{ord}(U), \operatorname{ord}(V) \leq r$ and coefficients of degree at most d. Show that computing $\operatorname{lclm}(U, V)$ costs no more than $\mathrm{O}^{\sim}(r^{\omega}d)$ operations in C.

Hint: Analyze the algorithm implicit in the proof of Theorem 4.30.

18*. Let $P \in C[x][\partial]$ and let $p \in C[x]$ be an irreducible factor of $\operatorname{lc}(P)$ such that p^k is removable at cost n from P, for some $k \in \mathbb{N}$. Show that there exist $e_0, \ldots, e_n \in \mathbb{N}$ and $q_0, \ldots, q_{n-1} \in C[x]$ with $\deg q_i < e_i \deg(p)$ $(i = 0, \ldots, n)$ such that

$$Q = \frac{1}{\sigma^n(p)^{e_n}}\partial^n + \frac{q_{n-1}}{\sigma^n(p)^{e_{n-1}}}\partial^{n-1} + \cdots + \frac{q_0}{\sigma^n(p)^{e_0}}$$

is a p^k-removing operator for P.

19*. Show that if $p_1, p_2 \in C[x]$ are removable at cost n from some operator $P \in C[x][\partial]$, then also $\operatorname{lcm}(p_1, p_2)$ is removable at cost n from P.

20. Analogous to right quotients, right remainders, right divisors, and left multiples, we can also define left quotients, left remainders, left divisors, and right multiples. Let $U = D^2 - (x^2 + 1)$, $V = xD^2 + (x^2 - 1)D - 2x \in C(x)[D]$.

a. Compute the greatest common left divisor of U and V.

b. Compute the least common right multiple of U and V.

21. Prove or disprove: $U, V \in K[\partial]$ have a nontrivial greatest common right divisor if and only if they have a nontrivial greatest common left divisor.

22. Can a recurrence have a d'Alembertian solution $\sum_{k=1}^{n} h_k$ for some hypergeometric term h_k without also having a hypergeometric solution similar to h_n?

References

Common right divisors and left multiples were already computed in the early days of differential and difference operators and noncommutative polynomial rings. Bostan, Chyzak, Li, and Salvy [88] trace back the history deeply into 19th century, so that Ore's paper from 1933 [344] almost seems recent. Even more recent is the exposition in the tutorial paper of Bronstein and Petkovšek [115]. The paper [88] contains a careful comparison of various algorithms for computing common left multiples.

Although the Gauss lemma does not literally hold in the case of Ore algebras, there is a theorem due to Kovacic [294, Proposition 2] which can be viewed as a version of the statement for differential operators.

Surgery on the Sylvester matrix is known as subresultant theory and was introduced into computer algebra by Collins [163] for improving the computation of polynomial gcds in the commutative case. The theory was adapted to the case of Ore polynomials by Li [308, 309]. Jaroschek [248, 249] uses Li's subresultants to speed up the computation of gcrd's in $K[\partial]$. Grigoriev [226] points out that the idea of subresultants can be extended to the case of more than two operators, and proposes an algorithm for computing the greatest common right divisor of several differential operators in polynomial time.

Part 2 of Theorem 4.30 belongs to a family of results concerning the more general phenomenon that we can sometimes get lower degree coefficients by allowing an operator to have higher degree. The relationships between orders and degrees are expressed as order-degree curves. The phenomenon was observed for the first time by Bostan, Chyzak, Salvy, Lecerf, and Schost for differential equations of algebraic functions [83]. The result discussed in Theorem 4.30 is taken from a paper of Kauers [265], which also contains results for other closure properties. Order-degree curves in the context of summation and integration are discussed in Sect. 5.5. A connection between order-degree curves and removability of singularities was observed by Chen, Jaroschek, Kauers, and Singer [136].

Bounds on the order n and the exponents e_i of a p-removing operator have been derived for the shift case by Abramov, Barkatou and van Hoeij [9, 24], and for the q-shift case by Koutschan and Zhang [292]. The pragmatic way to remove removable factors was studied by Chen, Kauers, and Singer [141], although it had been used long before this paper in internal parts of the Maple library. A refined version of removability, which also allows to remove constant factors, was proposed by Zhang [473, 474].

4.3 Several Functions

We have seen in Exercise 26 of Sect. 4.1 that the solutions f of an inhomogeneous equation $P \cdot f = g$ must be D-finite as soon as the inhomogeneous part g is D-finite. In this case, we have an equation $Q \cdot g = 0$ for some nonzero operator Q, and we can view the two equations $P \cdot f - g = 0$, $Q \cdot g = 0$ as a coupled system of two equations for two unknown functions. Every pair (f, g) of functions that forms a solution of this system will be such that both f and g are D-finite.

In this section we consider coupled systems of functional equations more systematically. For a fixed Ore algebra $K[\partial]$ and a $K[\partial]$-module F, we consider equations of the form

$$I_r\partial^m \cdot f + A_{m-1}\partial^{m-1} \cdot f + \cdots + A_0 \cdot f = 0$$

where $f = (f_1, \ldots, f_r) \in F^r$ is a vector of unknown functions, ∂ is understood to act componentwise on such vectors, i.e., $\partial \cdot f = (\partial \cdot f_1, \ldots, \partial \cdot f_r)$, and $A_0, \ldots, A_{m-1}$ are given elements of $K^{r\times r}$.

The first observation about such equations is that it suffices to consider the case $m = 1$, because we can always reduce to this situation at the cost of increasing the size of the matrices. An element f of F^r is a solution of the above equation if and only if the element $\tilde{f} = (f, \partial \cdot f, \ldots, \partial^{m-1} \cdot f)^T$ of F^{mr} is a solution of the matrix equation

$$\partial \cdot \tilde{f} = \begin{pmatrix} 0 & I_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & I_r \\ -A_0 & \cdots & \cdots & \cdots & -A_{m-1} \end{pmatrix} \tilde{f}.$$

The more interesting question concerns the opposite direction: instead of lowering the order of the equation at the cost of increasing the size of the matrices, can we also decrease the size of the matrices at the cost of increasing the order of the equations? According to the following proposition, the answer is yes.

Proposition 4.34 *Let $K[\partial]$ be an Ore algebra and F be a $K[\partial]$-module. Let $A \in K^{r\times r}$ and let $f = (f_1, \ldots, f_r) \in F^r$ be such that $(I_r\partial - A) \cdot f = 0$. Then each component f_i of f is D-finite.* □

Proof We show that there is an operator $P \in K[\partial] \setminus \{0\}$ such that $P \cdot f_i = 0$ for every i. Because of $\partial \cdot f = Af$, we have $\partial M \cdot f = (\sigma(M)A + \delta(M)) \cdot f$ for every $M \in K^{r\times r}$ (Exercise 1). Therefore, by induction, every vector $\partial^k \cdot f$ ($k \in \mathbb{N}$) belongs to the subspace $\{\, Mf : M \in K^{r\times r}\} \subseteq F^r$, whose dimension is at most $r \times r$. Consequently, the vectors $f, \partial \cdot f, \ldots, \partial^{r^2} \cdot f \in F^r$ are linearly dependent over K, so there are $p_0, \ldots, p_{r^2} \in K$, not all zero, such that $(p_0 + p_1\partial + \cdots + p_{r^2}\partial^{r^2}) \cdot f = 0$. ■

The argument used in the proof is somewhat brutal. It shows not only that each component f_i of a solution of the system is D-finite, but it constructs a single operator P that simultaneously annihilates every component f_i of any solution. This is more than we asked for, and as a result, the implied bound r^2 on the order of P is quite pessimistic. As we shall see later in this section, each component f_i is already annihilated by an operator of order at most r. On the other hand, knowing that there is an operator which annihilates all components of any solution of a coupled system offers us a quick alternative proof for some D-finite closure properties. For example, consider two D-finite functions $f, g \in F$, and suppose that $P \cdot f = Q \cdot g = 0$ for some $P, Q \in K[\partial] \setminus \{0\}$. Let $C_P \in K^{r\times r}$ and $C_Q \in K^{s\times s}$ be the companion matrices of P and Q, respectively, and consider the system

$$\partial \cdot h = \begin{pmatrix} C_P & \\ & C_Q \end{pmatrix} h.$$

Its solution space contains the vector $(f, g) \in F^2$, and so the operator which annihilates all components of (f, g) must annihilate both f and g. It must therefore annihilate $f + g$, thus showing that $f + g$ is D-finite.

In order to solve a given coupled system, it is not a good idea to work out the argument in the proof of Proposition 4.34. We can get along with shorter equations if we proceed more carefully.

Example 4.35 In order to solve the coupled system

$$\begin{aligned} f'(x) &= \frac{3x^2+4}{x(3x+2)} f(x) - \frac{6(x-2)}{x(3x+2)} g(x) \\ g'(x) &= \frac{3-x}{3x+2} f(x) + \frac{11}{3x+2} g(x), \end{aligned}$$

we can differentiate the first equation to get

$$\begin{aligned} f''(x) = {} & \frac{3x^2+4}{x(3x+2)} f'(x) + \frac{2(3x^2-12x-4)}{x^2(3x+2)^2} f(x) \\ & - \frac{6(x-2)}{x(3x+2)} g'(x) + \frac{6(3x^2-12x-4)}{x^2(3x+2)^2} g(x). \end{aligned}$$

Then we can use the second equation to eliminate $g'(x)$. This gives

$$f''(x) = \frac{3x^2+4}{x(3x+2)} f'(x) + \frac{2(3x^3-12x^2+6x-4)}{x^2(3x+2)^2} f(x) - \frac{12(4x^2-5x+2)}{x^2(3x+2)^2} g(x).$$

Finally, use the first equation to eliminate $g(x)$ and obtain

$$f''(x) = \frac{x^2-2}{x(x-2)} f'(x) - \frac{2(x-1)}{x(x-2)} f(x).$$

This equation has a solution space generated by x^2 and $\exp(x)$, and once we choose a solution $f(x) = \alpha x^2 + \beta \exp(x)$, the first equation forces us to set

$$g(x) = \left(\frac{3x^2+4}{x(3x+2)} f(x) - f'(x) \right) \frac{x(3x+2)}{6(x-2)} = -\frac{1}{2}\alpha x^3 - \frac{1}{3}\beta \exp(x).$$

The solution space of the coupled system is therefore generated by $(2x^2, -x^3)$ and $(3\exp(x), -\exp(x))$.

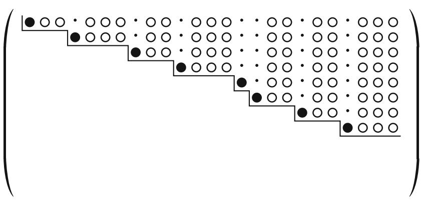
Note that we have found a second order equation for f and another equation that we may regard as a zeroth order inhomogeneous equation for g. The smallest operator that annihilates both f and g has order 3. □

The procedure applied in the example above can be viewed as a kind of Gaussian elimination applied to the matrix $I_r\partial - A \in K[\partial]^{r\times r}$. The usual Gaussian elimination turns a linear system over a field K into an equivalent linear system over K which has a particular structure, the essential property being that if the variables are $x_1, \dots, x_r$, then for every i there is at most one equation which contains x_i but none of $x_1, \dots, x_{i-1}$. Although $K[\partial]$ is not a field but a non-commutative ring, we can achieve the same structure for matrices with entries in $K[\partial]$.

Definition 4.36

1. A matrix $A \in K[\partial]^{r\times r}$ is called *(left) unimodular* if there exists a matrix $B \in K[\partial]^{r\times r}$ such that $BA = I_r$. Such a matrix B is then called a *left inverse* of A.
2. A matrix $A = ((a_{i,j}))_{i=1,j=1}^{r,s} \in K[\partial]^{r\times s}$ is said to be in *Hermite normal form* if
   a. For every $j \in \{1, \dots, s\}$ there is at most one $i \in \{1, \dots, r\}$ such that $a_{i,j} \neq 0$ and $a_{i,1} = \dots = a_{i,j-1} = 0$. For this i we have $\operatorname{lc}_\partial(a_{i,j}) = 1$.
   b. For every $(i, j) \in \{1, \dots, r\} \times \{1, \dots, s\}$ with $a_{i,j} \neq 0$ and $a_{i,1} = \dots = a_{i,j-1} = 0$ we have $a_{u,v} = 0$ for all $(u, v) \in \{i+1, \dots, r\} \times \{1, \dots, j-1\}$.
   c. For every $(i, j) \in \{1, \dots, r\} \times \{1, \dots, s\}$ with $a_{i,j} \neq 0$ and $a_{i,1} = \dots = a_{i,j-1} = 0$ we have $\operatorname{ord}(a_{1,j}), \dots, \operatorname{ord}(a_{i-1,j}) < \operatorname{ord}(a_{i,j})$.
3. A matrix $A \in K[\partial]^{r\times s}$ has a matrix $H \in K[\partial]^{r\times s}$ as Hermite normal form if H is a Hermite normal form and there is a left unimodular matrix U such that $UA = H$. □

The technical conditions in the definition of a Hermite normal form express that the matrix should have a staircase shape with zeros below the staircase and with the entries corresponding to a corner of the staircase having the largest order among all entries in their respective column.



Whenever a linear system of operator equations is in Hermite normal form, we can solve it from the bottom up, just like in linear algebra. For every corner position (i, j) in the staircase shape of the matrix, we have an inhomogeneous equation

$$a_{i,j} \cdot f_j = -a_{i,j+1} \cdot f_{j+1} - \cdots - a_{i,s} \cdot f_s$$

whose inhomogeneous part depends on functions $f_{j+1}, \ldots, f_s$ that either have already been determined (if there is a corner position corresponding to their index), or are "arbitrary functions" (if not).

Example 4.37

1. The matrix

$$H = \begin{pmatrix} D-1 & D \\ 0 & D^2 \end{pmatrix}$$

is in Hermite normal form. To solve the system $H \cdot (f_1, f_2)^T = 0$, we first solve $D^2 \cdot f_2 = 0$, which has a solution space generated by 1 and x. For a generic element $f_2 = c_1 + c_2 x$ of the solution space, we next solve the first equation $(D-1) \cdot f_1 = -D \cdot f_2 = c_2$. The space of all triples $(f_1, c_1, c_2) \in C[[x]] \times C^2$ satisfying this equation is generated by $(1, 0, 1)$, $(0, 1, 0)$, and $(\mathrm{e}^x, 0, 0)$. It follows that the solution space of the system $H \cdot (f_1, f_2)^T = 0$ is generated by $(1, x)$, $(0, 1)$, and $(\mathrm{e}^x, 0)$.

2. The matrix

$$H = \begin{pmatrix} D-1 & x & D \\ 0 & D & D^2 \end{pmatrix}$$

is also in Hermite normal form. We want to solve the system $H \cdot (f_1, f_2, f_3)^T = 0$. In this case, the matrix provides no equation for f_3, so we can let f_3 be an arbitrary element of $C[[x]]$. Let $a \in C[[x]]$ be arbitrary. For the choice $f_3 = a$, the component f_2 is determined through the inhomogeneous equation $D \cdot f_2 = -D^2 \cdot a$, whose general solution has the form $f_2 = c - a'$ for an arbitrary constant $c \in C$. Next we consider the equation $(D-1) \cdot f_1 + x f_2 + D \cdot f_3 = 0$. Plugging the general form of f_2 and the choice $f_3 = a$ into the equation leads to $(D-1) \cdot f_1 = -cx - (x+1)a'$. The homogeneous/parametric part $(D-1) \cdot f = -cx$ has a solution space generated by $(\mathrm{e}^x, 0)$ and $(x+1, 1)$ in $C[[x]] \times C$. The solutions of the inhomogeneous equation depend on the choice a and cannot be easily expressed in other terms. We can say however that for every choice a there is a certain $b \in C[[x]]$ such that the solution of the inhomogeneous equation is $f_1 = b + c_1 \mathrm{e}^x + c_2(x+1)$ for certain constants $c_1, c_2 \in C$. The solution set in $C[[x]]^3$ of the entire system $H \cdot (f_1, f_2, f_3)^T = 0$ can be described as

$$\Big\{ (b, a', a) + c_1(\mathrm{e}^x, 0, 0) + c_2(x+1, 1, 0) : \\ c_1, c_2 \in C, a \in C[[x]], \text{ and } b \text{ is such that } (D-1) \cdot b = (x+1)a' \Big\}.$$

Note that as a C-vector space, this solution set has infinite dimension. □

Faced with a system $A \cdot f = 0$ where $A \in K[\partial]^{r\times s}$ is not in Hermite normal form, we can exploit that for any unimodular matrix $U \in K[\partial]^{r\times r}$ we have $A \cdot f = 0 \iff UA \cdot f = 0$. The idea is thus to successively multiply A by a sequence of unimodular matrices so as to turn A into a Hermite normal form, and then solve the system as illustrated in the example above. This is of course the same general idea as in Gaussian elimination, where the elementary row operations play the role of the unimodular matrices, the only difference being that since $K[\partial]$ is not a field, we cannot simply divide a row by a nonzero matrix entry to produce an element by which all other elements of the column can be eliminated. But we can do division with remainder. If a column contains two nonzero entries, say $a, a' \in K[\partial]$ with $\operatorname{ord}(a) \le \operatorname{ord}(a')$, we can add the $-\operatorname{rquo}(a', a)$-fold of the row containing a to the row containing a'. This has the effect that a' gets replaced by $\operatorname{rrem}(a', a)$, which must have smaller order than a'. Doing the same computation for all rows in place of the row containing a', we can arrange that a becomes the element of largest order in the column under consideration. Now letting another nonzero entry of the column play the role of a (if there still is one), we can repeat the procedure to ensure that all other entries have strictly lower order. Since orders are natural numbers, we cannot observe infinitely many descents of the maximal order, so after finitely many repetitions we will reach a situation in which there is at most one nonzero entry left in the column. We have then found the first corner of the staircase. We then treat each of the remaining columns in the same way, except that the choice for a is limited to such rows which have no nonzero entries to the left of a. This leads to the following algorithm.

Algorithm 4.38
Input: $A = ((a_{i,j}))_{i=1,j=1}^{r,s} \in K[\partial]^{r\times s}$.
Output: *A Hermite normal form for* A.

Set $k = 1$.
for $j = 1, \ldots, s$ *do*
  while there are $i_1, i_2 \in \{k, \ldots, r\}$ *with* $i_1 \ne i_2$ *and* $a_{i_1,j}, a_{i_2,j} \ne 0$ *do*
    Choose i_1, i_2 *with* $a_{i_1,j}, a_{i_2,j} \ne 0$ *and* $\operatorname{ord}(a_{i_1,j}) \le \operatorname{ord}(a_{i_2,j})$.
    for $\ell = s, s-1, \ldots, j$ *do*
      $a_{i_2,\ell} = a_{i_2,\ell} - \operatorname{rquo}(a_{i_2,j}, a_{i_1,j}) a_{i_1,\ell}$.
  if there is an $i \in \{k, \ldots, r\}$ *with* $a_{i,j} \ne 0$ *then*
    Choose such an i *and swap the* i*th and* k*th row of* A.
    for $\ell = s, s-1, \ldots, j$ *do*
      $a_{k,\ell} = \operatorname{lc}(a_{k,j})^{-1} a_{k,\ell}$.
    for $i = 1, \ldots, k-1$ *and* $\ell = j, \ldots, s$ *do*
      $a_{i,\ell} = a_{i,\ell} - \operatorname{rquo}(a_{i,j}, a_{k,j}) a_{k,\ell}$.
    Set $k = k + 1$.
Return A.

Theorem 4.39 *Algorithm 4.38 is correct and terminates.* □

Proof For the termination, the only critical issue is the while loop starting in line 3. Within this loop, $a_{i_2,j}$ gets replaced by $a_{i_2,j} - \operatorname{rquo}(a_{i_2,j}, a_{i_1,j})a_{i_1,j} = \operatorname{rrem}(a_{i_2,j}, a_{i_1,j})$, whose order is strictly smaller than that of $a_{i_1,j}$. No entry of the jth column can get replaced by an element of higher order. The sum of the orders of the entries of the jth column is a natural number which decreases in every iteration. Since this cannot happen infinitely often, the loop must terminate.

For the correctness, note first that there is a unimodular matrix U such that multiplying U from the left to the input matrix produces the output matrix. This is because the matrix is only modified in lines 6, 8, 10 and 12, and the operations performed there correspond to left-multiplications by certain unimodular matrices (Exercise 7). The effect of the entire algorithm corresponds to the product of these matrices.

To show, secondly, that the output is a Hermite normal form, we show by induction on j that at the end of the jth iteration of the loop starting in line 2, the first j columns of A form a Hermite normal form whose first $k-1$ rows are nonzero. For the induction base $j = 1$ there is nothing to show. Suppose the claims are true for some $j-1$ and consider the jth iteration. As the while loop starting in line 3 only affects rows that have only zeros in the first $j-1$ columns, these operations do not affect any entries of these columns. In particular, the Hermite normal form structure of the first $j-1$ columns is preserved. After the while loop, the jth column contains at most one nonzero entry in rows $k, \ldots, r$. If it has none, the first j columns form a Hermite normal form with $k-1$ nonzero rows. If there is a nonzero entry, then after executing lines 8–12, the nonzero entry is in row k and monic, and all entries above have lower order. We have thus again a Hermite normal form with k nonzero rows. After updating the counter k in step 13, we have reached the claimed situation. ■

Example 4.40 Consider the matrix

$$A = \begin{pmatrix} D - \frac{3x^2+4}{x(3x+2)} & \frac{6(x-2)}{x(3x+2)} \\ -\frac{3-x}{3x+2} & D - \frac{11}{3x+2} \end{pmatrix} \in C(x)[D]^{2\times 2},$$

which corresponds to the system already considered in Example 4.35. We compute a Hermite normal form of A using Algorithm 4.38. The first column is cleaned up by adding the $(D - \frac{3x^2+4}{x(3x+2)})\frac{3x+2}{3-x}$-fold of the second row to the first (line 6), exchanging the two rows (line 8), and multiplying the second row by $-\frac{3x+2}{3-x}$ (line 10). The result is

$$\begin{pmatrix} 1 & \frac{3x+2}{x-3}D - \frac{11}{x-3} \\ 0 & \frac{-3x-2}{x-3}D^2 + \frac{(3x+2)(x^2-6)}{x(x-3)^2}D - \frac{3(x-2)(3x+2)}{x(x-3)^2} \end{pmatrix}.$$

After multiplying the second row by $\frac{x-3}{-3x-2}$, we obtain a Hermite normal form of A:

$$\begin{pmatrix} 1 & \frac{3x+2}{x-3}D - \frac{11}{x-3} \\ 0 & D^2 + \frac{6-x^2}{x(x-3)}D + \frac{3(x-2)}{x(x-3)} \end{pmatrix}.$$

□

According to its specification, Algorithm 4.38 computes "a" Hermite normal form for a given matrix in $K[\partial]^{r\times s}$. We show next that for every matrix in $K[\partial]^{r\times s}$ there is at most one Hermite normal form, so that we can meaningfully speak about "the" Hermite normal form of a matrix.

Proposition 4.41 *Let $H_1, H_2 \in K[\partial]^{r\times s}$ be two matrices in Hermite normal form, and suppose that there is a unimodular matrix $U \in K[\partial]^{r\times r}$ such that $UH_1 = H_2$. Then $H_1 = H_2$.* □

Proof We have to show that if there is a U such that $UH_1 = H_2$, we can choose $U = I_r$ as well. We proceed inductively along the structure of a Hermite normal form.

For the base case, note that $H_1 = 0$ if and only if $H_2 = 0$. More generally, the first column of H_1 is zero if and only if the first column of H_2 is. For the induction step, it therefore suffices to consider

$$H_1 = \begin{pmatrix} L_1 & P_1 \\ 0 & Q_1 \end{pmatrix} \quad \text{and} \quad H_2 = \begin{pmatrix} L_2 & P_2 \\ 0 & Q_2 \end{pmatrix},$$

with $L_1, L_2 \in K[\partial] \setminus \{0\}$, $P_1, P_2 \in K[\partial]^{1\times(s-1)}$, and $Q_1, Q_2 \in K[\partial]^{(r-1)\times(s-1)}$. By the induction hypothesis, we have $Q_1 = Q_2$. From $UH_1 = H_2$ we get $u_1 L_1 = e_1 L_2$, where u_1 is the first column of U and e_1 is the first unit vector. Coefficient comparison implies in succesion: all components of u_1 except for the first are zero, the first component of u_1 has order zero (otherwise U can't be invertible in $K[\partial]^{r\times r}$), $u_1 = e_1$ (using $\operatorname{lc}(L_1) = \operatorname{lc}(L_2)$), and finally $L_1 = L_2$.

We can thus conclude that $U = \begin{pmatrix} 1 & A \\ 0 & I_{r-1} \end{pmatrix}$ for some $A = (a_2, \dots, a_r) \in K[\partial]^{r-1}$ and it remains to show that we can take $A = 0$. Let $i \in \{2, \dots, r\}$.

Case 1: The ith row of H_1 is nonzero—say the first nonzero element is $M \in K[\partial]$ and appears in column j. Let h_1, h_2 be the jth columns of H_1, H_2, respectively. By the induction hypothesis, the vectors h_1, h_2 can only differ in their first components $h_{1,1}, h_{2,1}$. More precisely, we have $h_{1,1} + a_i M = h_{2,1}$, and since the structural requirements for a Hermite normal form require $\operatorname{ord}(h_{1,1}), \operatorname{ord}(h_{2,1}) < \operatorname{ord}(M)$, it follows that $a_i = 0$.

Case 2: The ith row of H_1 is zero. In this case, let j be arbitrary let h_1, h_2 be the jth columns of H_1, H_2 with $h_{1,1}, h_{2,1}$ as their (respective) first components. We then have $h_{1,1} + a_i 0 = h_{2,1}$, so $h_{1,1}$ and $h_{2,1}$ agree regardless of the choice of a_i and we may take $a_i = 0$. ■

Like for matrices over a field, we can draw some useful conclusions from Proposition 4.41. First of all, a matrix $A \in K[\partial]^{r\times r}$ is unimodular if and only if its Hermite normal form is I_r. Next, a matrix is unimodular if and only if it can be written as a product of elementary matrices (matrices corresponding to elementary row operations). Finally, since elementary matrices are both left and right unimodular, we find that every left-unimodular matrix is right-unimodular and vice versa, so there is no need to distinguish these notions.

The Hermite normal form has the advantage that we can solve higher order coupled linear systems directly, without having to translate them into first order systems with larger matrices. A disadvantage of the approach is that it is somewhat expensive. There is also an approach for solving linear systems of operator equations without increasing the order or the matrix sizes. Starting from a first order system $(I_r\partial - A)\cdot f = 0$ with $A \in K^{r\times r}$, the idea is to find a basis change that turns A into a companion matrix. If this can be done, the system naturally translates into an equation of order r with coefficients in K, and any solution of this equation can be translated back into a solution of the original system.

It must not be overlooked that the action of ∂ interferes with a basis change. If $P \in K^{r\times r}$ is an invertible matrix and we set $g = Pf$, then

$$\partial\cdot g = \partial\cdot Pf = \sigma(P)(\partial\cdot f) + \delta(P)f = \sigma(P)Af + \delta(P)f = (\sigma(P)A + \delta(P))P^{-1}g$$

so the basis change matrix P transforms the system $(I_r\partial - A)\cdot f = 0$ into the system $(I_r\partial - B)\cdot g = 0$ where $B = (\sigma(P)A + \delta(P))P^{-1} \in K^{r\times r}$. The matrix B is called the *gauge transform* of A with respect to P.

Definition 4.42 Let $K[\partial]$ be an Ore algebra and $P \in K^{r\times r}$ be an invertible matrix. For $A \in K^{r\times r}$, the matrix $P[A] := (\sigma(P)A + \delta(P))P^{-1}$ is called the *gauge transform* of A with respect to P. Two matrices $A, B \in K^{r\times r}$ are *gauge equivalent* if there exists an invertible matrix $P \in K^{r\times r}$ such that $P[A] = B$. □

Example 4.43

1. Continuing the previous example, let

$$A = \begin{pmatrix} \frac{3x^2+4}{x(3x+2)} & -\frac{6(x-2)}{x(3x+2)} \\ \frac{3-x}{3x+2} & \frac{11}{3x+2} \end{pmatrix} \in C(x)^{2\times 2}$$

and consider the system $(I_2D - A)\cdot f = 0$. With

$$P = \begin{pmatrix} 1 & 0 \\ \frac{3x^2+4}{x(3x+2)} & -\frac{6(x-2)}{x(3x+2)} \end{pmatrix} \in C(x)^{2\times 2}$$

we have

$$P[A] = \begin{pmatrix} 0 & 1 \\ -\frac{3(x-2)}{x(x-3)} & -\frac{6-x^2}{x(x-3)} \end{pmatrix}.$$

The matrix $P[A]$ is the companion matrix of the operator $D^2 + \frac{6-x^2}{x(x-3)}D + \frac{3(x-2)}{x(x-3)} \in C(x)[D]$. The solution x^2 of this operator gives rise to the solution $(x^2, 2x)$ of the coupled system $(I_2 D - P[A]) \cdot f = 0$, which in turn gives rise to the solution $P^{-1}(x^2, 2x) = (x^2, x^3/2)$ of the original system $(I_2 D - A) \cdot f = 0$. Likewise, the solution $\exp(x)$ of the operator translates into the solution $P^{-1}(\exp(x), \exp(x)) = (\exp(x), -\exp(x)/3)$.

2. For $L = D^2 - x \in C(x)[D]$, the module $C(x)[D]/\langle L\rangle$ is a $C(x)$-vector space of dimension 2. The sets $B_1 = \{1, D\}$ and $B_2 = \{x + D, x - D\}$ are bases of this vector space. For transforming a B_1-representation of some element of $C(x)[D]/\langle L\rangle$ into a B_2-representation of the same element, we do *not* need a gauge transform. Instead, this is a matter of the usual matrix-vector multiplication from linear algebra. □

Given an arbitrary matrix $A \in K^{r\times r}$, our goal is to find an invertible matrix $P \in K^{r\times r}$ such that $P[A]$ has the form of a companion matrix. Suppose $P \in K^{r\times r}$ is such a matrix, i.e., such that $P[A] = (\sigma(P)A + \delta(P))P^{-1} = C_L$, where

$$C_L = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ * & \cdots & \cdots & \cdots & * \end{pmatrix} \in K^{r\times r}$$

is the companion matrix of some operator $L \in K[\partial]$. We then have $\sigma(P)A+\delta(P) = C_L P$, and by the shape of a companion matrix, the ith row of $C_L P$ is equal to the $(i+1)$st row of P, for $i = 1, \ldots, r-1$. At the same time, if we know the ith row of P, we can compute from it the ith row of $\sigma(P)A + \delta(P)$, so if we have $\sigma(P)A + \delta(P) = C_L P$, we can compute the $(i+1)$st row of P from the ith row of P, for every $i = 1, \ldots, r-1$. In other words, it suffices to determine the first row of a suitable transformation matrix P. The remaining rows of P are uniquely determined.

Conversely, let $p \in K^r$ be any vector (viewed as a row vector) and consider the matrix $P \in K^{r\times r}$ whose rows are $p_1, \ldots, p_r \in K^r$ defined by $p_1 = p$ and $p_{i+1} = \sigma(p_i)A + \delta(p_i)$ $(i = 1, \ldots, r-1)$. We then have

$$\begin{pmatrix} \sigma(p_1) \\ \vdots \\ \vdots \\ \sigma(p_{r-1}) \end{pmatrix} A + \begin{pmatrix} \delta(p_1) \\ \vdots \\ \vdots \\ \delta(p_{r-1}) \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}}_{\in K^{(r-1)\times r}} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ \vdots \\ p_r \end{pmatrix},$$

and it remains to check whether there is some vector $u \in K^r$ which we can use as an additional rth row in the first matrix on the right so that the left hand side gains $\sigma(p_r)A + \delta(p_r)$ as an rth row. The question amounts to an inhomogeneous linear system for the unknown vector u, and since we are only interested in situations where P is invertible, we can be sure that a unique vector u exists.

Whether P is invertible depends on the choice of its first row p. A vector $p \in K^r$ is called *cyclic* (with respect to A, σ, δ) if the matrix $P \in K^{r\times r}$ constructed as described above is invertible. Equivalently, p is cyclic if and only if the vectors $p_1, \dots, p_r \in K^r$ form a basis of K^r. We could now proceed to argue that almost all vectors are cyclic and propose a randomized algorithm that picks candidates at random until a cyclic vector is encountered. Some implementations proceed like this. In fact, it is not really so dramatic if we accidentally encounter a non-cyclic vector. If p is not cyclic, i.e., if $p_1, \dots, p_r \in K^r$ do not form a basis of K^r, then there is some $i < r$ such that $p_1, \dots, p_i$ are linearly independent but $p_{i+1} = \sigma(p_i)A + \delta(p_i)$ is a K-linear combination of $p_1, \dots, p_i$. We can adjust the definition of the vectors $p_1, p_2, \dots$ by setting $p_{i+1} = \sigma(p_i)A + \delta(p_i)$ only if this vector does not belong to the K-linear subspace of K^r generated by $p_1, \dots, p_i$, and otherwise setting p_{i+1} to an arbitrary vector that does not belong to the subspace generated by $p_1, \dots, p_i$. With this definition, it is clear that the resulting vectors $p_1, \dots, p_r$ will be a basis of K^r, and if $P \in K^{r\times r}$ is the matrix which has $p_1, \dots, p_r$ as rows, then we have $\sigma(P)A + \delta(P) = A'P$ for some matrix $A' \in K^{r\times r}$ which has the form

$$A' = \left(\begin{array}{c|c|c|c}
\left.\begin{matrix}0&1&&\\&\ddots&\ddots&\\&&0&1\\ *&\cdots&\cdots&*\end{matrix}\right\}r_1\times r_1 & & & \\ \hline
\begin{matrix}0&\cdots&\cdots&0\\ \vdots&&&\vdots\\0&\cdots&\cdots&0\\ *&\cdots&\cdots&*\end{matrix} & \left.\begin{matrix}0&1&&\\&\ddots&\ddots&\\&&0&1\\ *&\cdots&\cdots&*\end{matrix}\right\}r_2\times r_2 & & \\ \hline
\multicolumn{2}{c|}{\begin{matrix}0&\cdots&\cdots&\cdots&\cdots&0\\ \vdots&&&&&\vdots\\0&\cdots&\cdots&\cdots&\cdots&0\\ *&\cdots&\cdots&\cdots&\cdots&*\end{matrix}} & \begin{matrix}0&1&&\\&\ddots&\ddots&\\&&0&1\\ *&\cdots&\cdots&*\end{matrix} & \\ \hline
&&&\ddots
\end{array}\right).$$

This is in general not a companion matrix, but it is close enough. If there are m companion-like blocks in A' of respective sizes $r_1, \dots, r_m$, then the system $(I_r\partial - A') \cdot f = 0$ translates into a system

$$\begin{aligned}
L_1 \cdot f_1 &= 0\\
L_2 \cdot f_2 &= M_{2,1} \cdot f_1\\
&\ \vdots
\end{aligned}$$

$$L_m \cdot f_m = M_{m,1} \cdot f_1 + \cdots + M_{m,m-1} \cdot f_{m-1}$$

in which $L_1, \ldots, L_m \in K[\partial]$ are known operators of respective orders $r_1, \ldots, r_m$, the $M_{i,j} \in K[\partial]$ are known operators of order $< r_j$, and $f_1, \ldots, f_m$ are unknown scalar functions. The system is uncoupled in the sense that we can solve it if we know how to solve (inhomogeneous) scalar equations.

If we choose the kth unit vector as the first p, then the resulting operator L_1 corresponding to the first block will be an annihilating operator for the kth component of any solution vector $f \in K^r$ of the original system $(I_r\partial - A) \cdot f = 0$. Since $\operatorname{ord}(L_1) \leq r$, we see that each component of a solution vector of such a system is D-finite of order at most r. This refines the bound obtained in Proposition 4.34.

The uncoupling algorithm described above can be summarized as follows:

Algorithm 4.44
Input: *$A \in K^{r\times r}$, an endomorphism $\sigma\colon K \to K$, and a σ-derivation $\delta\colon K \to K$.*
Output: *An invertible matrix $P \in K^{r\times r}$ such that $P[A]$ has the shape described above.*

1 *Set $P = 0 \in K^{r\times r}$ and $k = 0$.*
2 *while $k < r$ do*
3 *Choose a vector $p \in K^{r\times r} \setminus \{0\}$ and set the $(k+1)$st row of P to p.*
4 *for $i = 2, \ldots, r-k$ do*
5 *Set $p = \sigma(p)A + \delta(p)$ and set the $(k+i)$th row of P to p.*
6 *Set k to be the largest number such that the first k rows of P are linearly independent over K.*
7 *Return P.*

Theorem 4.45

1. *Algorithm 4.44 is correct.*
2. *Suppose that $K = C(x)$ and σ, δ map polynomials to polynomials with $\deg\sigma(p), \deg\delta(p) < \deg p$ for all $p \in C[x]$, and suppose that the application of σ and δ to a polynomial of degree d costs no more than $\mathrm{O}^{\sim}(d)$ operations in C. For this setting, Algorithm 4.44 can be implemented in such a way that whenever it is applied to any matrix $A \in C[x]^{r\times r}$ with entries of degree at most d, it performs no more than $\mathrm{O}^{\sim}(r^{\omega+2}d)$ operations in C.* □

Proof

1. That P is invertible follows from the choice of k in line 6 and the termination condition in line 2. That $P[A]$ has the required form follows from the discussion above. This implies the correctness of the algorithm.
2. We need to be more specific about the implementation of lines 3 and 6. If in line 3 we always choose a vector with entries in C, then P will always be a matrix with entries of degree at most rd.
   For line 6, we can apply a bisection search to find k such that the top k rows of P form a matrix of rank k. This takes at most $\log(k)$ rank computations,

each of which can be done with at most $O^{\sim}(r^{\omega}rd)$ operations in C according to Theorem 1.28. Since $\log(k) \leq \log(r)$, identifying k also costs $O^{\sim}(r^{\omega}rd)$ operations. If k increases in each iteration of the loop, the total cost contributed by line 6 amounts to $O^{\sim}(r^{\omega+2}d)$ operations.

In order to ensure that k increases in each loop iteration, we should choose in line 3 a vector p which does not belong to the vector space generated by the first k rows of P. One way of doing so is to maintain a pool of candidates, which is initially set to the set of all the unit vectors $e_1, \ldots, e_r$. In line 3, we select an element from the pool and test whether it is linearly independent with the first k rows of P. This costs $O^{\sim}(r^{\omega}rd)$ operations. If it is linearly dependent, it will always be, so we can safely remove it from the pool and try another element. Once we find an element that is linearly independent, we take it as p and remove it from the pool. Since the r vectors initially in the pool form a basis of K^r, we will never run out of candidates. Moreover, we will altogether at most r times check whether a pool element is suitable, so the total number of operations spent in line 3 can be limited to $O^{\sim}(r^{\omega+2}d)$.

With the assumptions on σ and δ, each execution of line 5 costs $O^{\sim}(r^2d)$ operations, so each execution of the loop in lines 4 and 5 amounts to $O^{\sim}(r^3d)$ operations, and the total cost to $O^{\sim}(r^4d)$. Since $\omega \geq 2$, this is bounded by $O^{\sim}(r^{\omega+2}d)$ operations. ■

Algorithm 4.44 pays a price for being a deterministic algorithm. If we are willing to turn it into a randomized algorithm, we could simply let it choose a random element of K^r as p, build a candidate transformation matrix P from it, and check whether it is invertible. With high probability, this will be the case. If it is not the case, we can either return "failed" or try again, depending on whether we prefer a Monte Carlo or a Las Vegas style randomized algorithm. Either way, the expected runtime drops to $O^{\sim}(r^{\omega+1}d)$ for the setting described in part 2 of Theorem 4.45.

Being deterministic, Algorithm 4.44 has the feature that we can also choose simple vectors as p in line 3, which might not qualify as honest random elements of K^r. This way, we can keep the degrees of the entries in P low.

Coupled systems of functional equations arise naturally in a number of contexts. As an example, let $K[\partial]$ be an operator and $L_1, L_2 \in K[\partial]$ be two elements of some order r, and consider the corresponding quotient modules $M_1 = K[\partial]/\langle L_1\rangle$ and $M_2 = K[\partial]/\langle L_2\rangle$. Given L_1, L_2, how can we decide whether M_1 and M_2 are isomorphic as $K[\partial]$-modules? Since the module M_1 is generated by [1], a module homomorphism $h\colon M_1 \to M_2$ is uniquely determined by an operator $U \in K[\partial]$ such that $h([1]) = [U] \in M_2$. For more clarity, instead of the generic equivalence class notation $[P]$, we will write $[P]_{L_i}$ for the class of P modulo L_i, so that $[P]_{L_i}$ is more easily recognized as an element of M_i ($i = 1, 2$). For any other operator $P \in K[\partial]$ we have

$$[PU]_{L_2} = P \cdot [U]_{L_2} = P \cdot h([1]_{L_1}) = h(P \cdot [1]_{L_1}) = h([P]_{L_1}).$$

In order for h to be well-defined, we must ensure that the zero of M_1 is mapped to the zero of M_2, i.e., that $h([0]_{L_1}) = h([L_1]_{L_1}) = [L_1 U]_{L_2} = [0]_{L_2}$, i.e., that $L_1 U = V L_2$ for some $V \in K[\partial]$. We can search for U and V simultaneously by making an ansatz $U = u_0 + \cdots + u_{r-1}\partial^{r-1}$, $V = v_0 + \cdots + v_{r-1}\partial^{r-1}$ and equate the coefficients of $L_1 U - V L_2$ to zero. This looks similar to the computation of least common left multiples, but observe that U is now to the right of L_1 rather than to the left. By commuting the powers of ∂ appearing in L_1 with the undetermined coefficients of U, we introduce derivations of these, so that the coefficient comparison does not simply result in a linear system over K but in a system of functional equations.

The solutions of the functional equations give rise to the choices of U that lead to well-defined homomorphisms from M_1 to M_2. In order to decide the isomorphism question, it remains to check whether any of these homomorphisms is surjective. For a specific choice U, this is the case if and only if the elements $[\partial^i U]_{L_2}$ ($i = 0, \ldots, r-1$) are linearly independent over K, which is easy to check with linear algebra. The set of all possible choices U forms a finite-dimensional C-vector space, generated by $U_1, \ldots, U_m$. In order to check whether this space contains an element that corresponds to an isomorphism, consider a linear combination $U = c_1 U_1 + \cdots + c_m U_m$ with undetermined coefficients $c_1, \ldots, c_m$ and use linear algebra to find out whether the elements $[\partial^i U]_{L_2}$ ($i = 1, \ldots, r-1$) are linearly dependent for every choice of $c_1, \ldots, c_m$. This is the case if and only if there is no isomorphism.

Example 4.46

1. Let $L_1 = D^2 - x$ and $L_2 = (1-x)D^2 + D + (x^2 - x - 1)$, and consider the modules $M_1 = C(x)[D]/\langle L_1\rangle$ and $M_2 = C(x)[D]/\langle L_2\rangle$. For deciding whether $M_1 \cong M_2$ as $C(x)[D]$-modules, we make an ansatz

$$(D^2 - x)(u_0 + u_1 D) - (v_0 + v_1 D)((1-x)D^2 + D + (x^2 - x - 1)) = 0$$

with undetermined coefficients $u_0, u_1, v_0, v_1 \in C(x)$. Expanding and collecting terms gives

$$\begin{aligned}&\big(u_0'' - xu_0 + (-x^2 + x + 1)v_0 + (1-2x)v_1\big)\\ &+ \big(2u_0' + u_1'' - xu_1 - v_0 + (-x^2 + x + 1)v_1\big)D\\ &+ \big(u_0 + 2u_1' + (x-1)v_0\big)D^2 + \big(u_1 + (x-1)v_1\big)D^3 = 0.\end{aligned}$$

By equating the coefficients of D^2 and D^3 to zero, we can solve for v_0, v_1 in terms of u_0, u_1, u_1', and plugging these expressions into the coefficients of D^0 and D^1 gives a coupled system of differential equations for u_0 and u_1:

$$\begin{aligned}&(x-1)u_0'' + 2(x^2 - x - 1)u_1' - u_0 + (2x-1)u_1 = 0,\\ &(x-1)u_1'' + 2(x-1)u_0' + u_0 + 2u_1' - u_1 = 0.\end{aligned}$$

With the methods described in this section, we can determine the solution space of this system. It turns out to be generated by $(u_0, u_1) = (\frac{1}{1-x}, \frac{1}{1-x}) \in C(x)^2$. It remains to check whether for $U = \frac{1}{1-x}(1 + D)$ the operators $\operatorname{rrem}(U, L_2)$ and $\operatorname{rrem}(DU, L_2)$ are linearly independent over $C(x)$. Since they are, it follows that M_1 and M_2 are isomorphic.

2. Now let $L_1 = D^2 - (x + 1)D + x$ and $L_2 = (2 - x^2)D^2 + 2xD + (x^2 - 6)$, and consider the modules $M_1 = C(x)[D]/\langle L_1\rangle$ and $M_2 = C(x)[D]/\langle L_2\rangle$. In this case, the ansatz $L_1(u_0 + u_1 D) - (v_0 + v_1 D)L_2 = 0$ leads to a system of equations which, after eliminating v_0 and v_1, reads

$$
\begin{aligned}
&(x^2 - 2)u_0'' - (x + 1)(x^2 - 2)u_0' + (x^3 + x^2 - 2x - 6)u_0\\
&\qquad + (2x^2 - 6)u_1' - (x + 3)(x^2 - 2x - 2)u_1 = 0,\\
&(2x^2 - 2)u_0' + (-x^3 - x^2 + 4x + 2)u_0\\
&\qquad + (x^2 - 2)u_1'' + (-x^3 - x^2 + 6x + 2)u_1' + (x^3 - x^2 - 4x - 4)u_1 = 0.
\end{aligned}
$$

Its solution space is generated by $(u_0, u_1) = (\frac{x-2}{x^2-2}, \frac{x-1}{x^2-2})$, but for $U = \frac{x-2}{x^2-2} + \frac{x-1}{x^2-2}D$ we have $\operatorname{rrem}(DU, L_2) = U$, which is obviously linearly dependent with U. It follows that although there is a nontrivial homomorphism from M_1 to M_2, the modules are not isomorphic.

3. For $L_1 = D^2 - x$ and $L_2 = D^2 + x$ the resulting coupled system has only the solution $(u_0, u_1) = (0, 0)$, so in this case, there is no nontrivial homomorphism from $C(x)[D]/\langle L_1\rangle$ to $C(x)[D]/\langle L_2\rangle$. □

In order to solve a coupled system, we uncouple it so that algorithms from earlier chapters become applicable. We have seen that one way of uncoupling is to apply a suitable gauge transformation to the system. Gauge transformations are not only useful for uncoupling, but they can also be used to study other aspects of the system at hand. For example, gauge transformations are used for extending the definition of removable singularities to systems, and for detecting them. For simplicity, let us restrict to the shift case. In this case, an element of $C/\mathbb{Z}$ is called a *singularity* of a system $(I_r S - A) \cdot f = 0$ with $A \in C(x)^{r\times r}$ if it contains a pole of an entry of A. A singularity is called *removable* if there is a polynomial matrix $P \in C[x]^{r\times r}$ with nonzero determinant (so that it is invertible as element of $C(x)^{r\times r}$) such that $P[A]$ does not have this singularity.

Example 4.47 Let

$$A = \begin{pmatrix} \frac{3x^3-4x^2-2x-2}{x(x+1)} & -\frac{x^3-7x^2-2x-2}{2x(x+1)} \\ \frac{2(3x^3-4x^2-x-1)}{x(x+1)} & -\frac{2x^3-6x^2-x-1}{x(x+1)} \end{pmatrix} \in C(x)^{2\times 2}$$

and consider the system $(I_2 S - A) \cdot f = 0$. Its only singularity is the class $\mathbb{Z} \in C/\mathbb{Z}$. To see whether it is removable, we first try to eliminate the factors $x + 1$ and then the factors x from the denominators. Useful gauge transforms to this end are constant matrices and diagonal matrices with polynomial entries. Using constant matrices, we can try to remove poles by applying suitable linear combinations to the rows and columns of the matrix at hand. For example, since

$$[(x+1)^{-1}]A = \begin{pmatrix} 7 & -4 \\ 14 & -8 \end{pmatrix},$$

we can make some progress by adding the (-2)-fold of the first row to the second. Note that this has the side effect that the 2-fold of second column gets added to the first, but this will not spoil the desired elimination effect.

$$P_1 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \quad \Rightarrow \quad A_1 := \sigma(P_1)AP_1^{-1} = \begin{pmatrix} \frac{x(2x+3)}{x+1} & -\frac{x^3-7x^2-2x-2}{2x(x+1)} \\ -2x & -\frac{x^2+1}{x} \end{pmatrix}.$$

We have successfully removed the factor $x+1$ from the denominators of the second row. To remove them also from the first row, we can simply multiply this row by $x+1$. This has the side effect that the first column will be divided by x, but we are lucky that x appears in all numerators of the first column, so that no new denominators get introduced. If this were not the case, we would nevertheless proceed in the same way, because we will also have to deal with the denominators x in the second column.

$$P_2 = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \quad \Rightarrow \quad A_2 := \sigma(P_2)A_1P_2^{-1} = \begin{pmatrix} 2x+3 & -\frac{x^3-7x^2-2x-2}{2x} \\ -2 & -\frac{x^2+1}{x} \end{pmatrix}.$$

To get rid of the remaining denominators, considering

$$[x^{-1}]A_2 = \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}$$

suggests adding the first column to the second. This gives

$$P_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \Rightarrow \quad A_3 := \sigma(P_3)A_2P_3^{-1} = \begin{pmatrix} \frac{(x-1)(x^2-2x+2)}{2x} & -\frac{x^3-7x^2-2x-2}{2x} \\ \frac{1}{2}(x-1)x & \frac{1}{2}(-x^2+5x+2) \end{pmatrix},$$

from which we clear denominators by multiplying the first row with x:

$$P_4 = \begin{pmatrix} x-1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \quad A_4 := \sigma(P_4)A_3P_4^{-1} = \begin{pmatrix} \frac{1}{2}(x^2-2x+2) & \frac{1}{2}(-x^3+7x^2+2x+2) \\ \frac{x}{2} & \frac{1}{2}(-x^2+5x+2) \end{pmatrix}.$$

Since we have reached a matrix with polynomial entries, the singularity $\mathbb{Z}$ of A is removable. The matrix $P = P_4P_3P_2P_1 \in C[x]^{2\times 2}$ is a gauge transform which removes the singularity from A. □

Exercises

1. Let $K[\partial]$ be an Ore algebra. Show that $K^{r\times r}[\partial]$ is an Ore algebra if σ and δ are defined entry-wise by the σ and δ of $K[\partial]$.

2. Let $K[\partial]$ be an Ore algebra and $A \in K^{r\times r}$ be invertible. Show: **a.** $\sigma(A^{-1}) = \sigma(A)^{-1}$; **b.** $\delta(A^{-1}) = -\sigma(A^{-1})\delta(A)A^{-1}$.

3. Consider the Ore algebra $C[\partial]$ (i.e., $\sigma = \mathrm{id}$ and $\delta = 0$). Show that for every $A \in C^{r\times r}$ there is an operator $L \in C[\partial]$ of order at most r such that every component of a solution $f \in F^r$ of the system $(I_r\partial - A)\cdot f = 0$ is annihilated by L. This refines the bound of Proposition 4.34 for this particular situation.

4. Show that for every $r \in \mathbb{N}$ there exists a matrix $A \in C(x)^{r\times r}$ such that every operator $L \in C(x)[D]\setminus\{0\}$ which annihilates each component of a solution $f \in F^r$ of the system $(I_rD - A)\cdot f = 0$ has order at least r^2.

5***.** In the shift case, reprove that D-finiteness is preserved under multiplication using Proposition 4.34.

6. Show that $\begin{pmatrix} S+1 & S^2 - x(x+2)S + x \\ 1 & S - x^2 \end{pmatrix} \in C(x)[S]^{2\times 2}$ is unimodular.

7. **a.** Show that every invertible matrix $A \in K^{r\times r}$ is unimodular as an element of $K[\partial]^{r\times r}$.

b. Let $r \in \mathbb{N}$, $u, v \in \{1,\dots,r\}$, $u \neq v$, and let $L \in K[\partial]$. Let $A = ((a_{i,j}))_{i,j=1}^r \in K[\partial]^{r\times r}$ be defined by $a_{u,v} = L$ and $a_{i,j} = \delta_{i,j}$ when $(i,j) \neq (u,v)$. Show that A is unimodular.

8. Find all solutions in $C(x)^3$ of the following systems:

a. $$\Bigl(I_3S - \tfrac{1}{2x(1+x)}\begin{pmatrix} x(2x+1) & -4x(x+1) & -1 \\ 0 & -2x(x+1) & 0 \\ -x(x+1) & 4x(x+1)^2 & (x+1)(2x+1) \end{pmatrix}\Bigr)\cdot f = 0$$

b. $$\Bigl(I_3D - \tfrac{1}{2x^2}\begin{pmatrix} -x & x^2 & -1 \\ 0 & 2x^2 & 0 \\ -x^2 & -x^3 & x \end{pmatrix}\Bigr)\cdot f = 0$$

9. Construct a matrix $A \in C(x)^{3\times 3}$ so that the solution space of the system $(I_3D - A)\cdot f = 0$ in $C(x)^3$ is generated by $\begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix}, \begin{pmatrix} 1 \\ x+1 \\ (x+1)^2 \end{pmatrix}, \begin{pmatrix} 1 \\ x+2 \\ (x+2)^2 \end{pmatrix}$.

10. Let $A \in K[\partial]^{r\times 1} \setminus \{0\}$ and let H be the Hermite normal form of A. Show that $H = (G, 0, \dots, 0)^T$ where $G \in K[\partial]$ is the greatest common right divisor of the entries of A.

11. In this section, we have only discussed homogeneous systems $(I_r\partial - A)\cdot f = 0$. We want to adapt the methods to solve parameterized inhomogeneous systems $(I_r\partial - A)\cdot f = c_1 g_1 + \cdots + c_m g_m$ where $A \in K^{r\times r}$ and $g_1, \dots, g_m \in K^r$ are given and $f \in K^r$ and $c_1, \dots, c_m \in C$ are unknown. How can we do this **a.** using the Hermite normal form; **b.** using Algorithm 4.44?

12***.** Show that gauge equivalence is an equivalence relation.

13. Design an algorithm for the differential case with $K = C(x)$ that decides whether two given matrices A, B are gauge equivalent.

14****.** Prove or disprove:
  a. Any two gauge equivalent systems have the same solution space.
  b. Any two companion matrices which are gauge equivalent are in fact equal.
  c. For $A = I_r$ there is no cyclic vector when $r \geq 2$.

15. Show that whenever $A \in K^{r\times r}$ is a companion matrix, e_1 is a cyclic vector. Find a matrix $A \in K^{r\times r}$ which is not a companion matrix but for which e_1 is nevertheless a cyclic vector.

16. Let $L \in K[\partial]$ with $r = \operatorname{ord}(L) > 0$ and let $C_L \in K^{r\times r}$ be the companion matrix of L. Show that the definition $\partial \cdot p := \sigma(p)C_L + \delta(p)$ turns the K-vector space K^r into a $K[\partial]$-module which is isomorphic to $K[\partial]/\langle L\rangle$.

17***.** Let $K[\partial]$ be an Ore algebra and F be a $K[\partial]$-module such that for every $L \in K[\partial]$ of order r the solution space $V(L)$ has dimension at most r (as vector space over C). Show that for every $A \in K^{r\times r}$ the solution space of the system $(I_r\partial - A)\cdot f = 0$ in F^r has dimension at most r (as vector space over C).

18***.** Show that for every $A \in C[[x]]^{r\times r}$ the system $(I_r D - A)\cdot f = 0$ has r linearly independent solutions in $C[[x]]^r$.

19***.** Let $A = \begin{pmatrix} 0 & 1/x \\ 0 & 0 \end{pmatrix} \in C(x)^{2\times 2}$. Show that 0 is not a removable singularity in the differential case.

Hint: Consider the solutions of the system $(I_2 D - A)\cdot f = 0$ and use the results of the previous two exercises.

20****.** Gauge transformations can be defined not only for matrices, but also for operators. For $P, A \in K[\partial]$ with $\operatorname{lc}(P) = 1$, the operator $P[A] := \operatorname{rquo}(\operatorname{lclm}(P, A), P) \in K[\partial]$ is called the *gauge transform* of A with respect to P. Suppose that $K[\partial]$ acts on a module F such that $\dim V(L) = \operatorname{ord}(L)$ for every $L \in K[\partial]$. Show the following properties of the gauge transform:
  a. $V(P[A]) = P \cdot V(A)$ (in other words, P acts as a C-vector space isomorphism from $V(A)$ to $V(P[A])$).
  b. $P[\operatorname{lclm}(A, B)] = \operatorname{lclm}(P[A], P[B])$.
  c. $\operatorname{gcrd}(P, A) = 1 \iff \operatorname{ord}(A) = \operatorname{ord}(P[A])$.

21****.** The Bessel function $J_\nu(x)$ satisfies the differential equation $x^2 J_\nu''(x) + x J_\nu'(x) + (x^2 - \nu^2) J_\nu(x) = 0$. Solve the differential equation

$$x(2x-1)(10x+9)f''(x)+2(50x^2+39x-18)f'(x)+(20x^3+8x^2-3x+99)f(x) = 0$$

in terms of Bessel functions. More precisely, find $u, v \in C(x)$ such that $f(x) = u(x)J_2(x) + v(x)J_2'(x)$ is a solution.

22. Design an integration algorithm for algebraic functions. More precisely, for a given algebraic extension $K = C(x)[y]/\langle m\rangle$ of $C(x)$ and a given element $f \in K$, the algorithm shall decide whether there exists a $g \in K$ such that $g' = f$ (i.e., $\int f = g$).

Hint: Recall that K is a finite-dimensional $C(x)$-vector space.

23. A sequence $(p_n)_{n=0}^\infty$ is called a *quasi-polynomial* if there is a root of unity $\omega \in C$, say of order $k \in \mathbb{N}$, and polynomials $p_0, \ldots, p_{k-1} \in C[x]$ such that $p_n = p_0(n)+\omega^n p_1(n)+\cdots+\omega^{(k-1)n} p_{k-1}(n)$ for all $n \in \mathbb{N}$. Let $(p_n^{(0)})_{n=0}^\infty, \ldots, (p_n^{(r)})_{n=0}^\infty$ be quasi-polynomials and suppose that the sequence $(a_n)_{n=0}^\infty$ satisfies the recurrence

$$p_n^{(0)} a_n + p_n^{(1)} a_{n+1} + \cdots + p_n^{(r)} a_{n+r} = 0$$

for all $n \in \mathbb{N}$. Show that $(a_n)_{n=0}^\infty$ is D-finite.

References

Algorithm 4.38 is perhaps the most straightforward algorithm for computing the Hermite normal form, but it is certainly not the most efficient one. A less straightforward but more efficient algorithm was proposed by Giesbrecht and Kim [215]. Their algorithm only requires a polynomial number of operations in the constant field C.

Churchill and Kovacic [152] prove in a fairly general setting that cyclic vectors always exist, and that in fact almost every vector is cyclic. Their paper contains references to several earlier proofs. While the cyclic vector method is the oldest way to uncouple systems, it was long considered not satisfactory, so alternative methods were developed, for example by Barkatou [41], by Zürcher [477] and by Abramov and Zima [20]. Bostan, Chyzak and de Panafieu [92] somewhat rehabilitated the cyclic vector approach by a careful complexity analysis.

Our main motivation for uncoupling algorithms is that we want to apply the algorithms from Chaps. 2 and 3 to find the solution of systems. It is also possible to compute such solutions directly, without first transforming the given system into a scalar equation. Such algorithms were developed by Barkatou [42] for the differential case and by Abramov and Barkatou [8] for the recurrence case. These algorithms have been implemented as Maple package ISOLDE by Barkatou and

Pflügel. The analysis of removable singularities sketched at the end of the section is another example for a problem that can be solved without uncoupling. Complete desingularization algorithms for systems were given by Barkatou and Maddah [45] for the differential case, and by Barkatou and Jaroschek [43, 44] for the shift case.

4.4 Factorization

If $f \in F$ is annihilated by some operator $L \in K[\partial]$, then it is also annihilated by every left multiple ML of L, because $(ML)\cdot f = M\cdot(L\cdot f) = M\cdot 0 = 0$. Conversely, if we are interested in "simple" solutions of a given operator $L \in K[\partial]$, we could try to write the operator as a product $L = L_1 L_2$ of two operators $L_1, L_2 \in K[\partial]$, because every solution of L_2 will also be a solution of L. We have already done so in Sects. 2.6 and 3.6, when we searched for hypergeometric or hyperexponential solutions of a given equation. We have seen that such solutions correspond to right factors of order 1. If there are no hypergeometric or hyperexponential solutions, i.e., no right factors of order 1, the next natural question is whether there are right factors of higher order. In the present section we discuss how this question can be answered.

Definition 4.48 An operator $L \in K[\partial] \setminus K$ is called *irreducible* if for any $P, Q \in K[\partial]$ with $L = PQ$ we have $\operatorname{ord}(P) = 0$ or $\operatorname{ord}(Q) = 0$. If it is not irreducible, it is called *reducible.* □

As in the case of commutative polynomial rings, every operator $L \in K[\partial] \setminus K$ can be written as a product of finitely many irreducible factors. However, unlike in the commutative case, the factorization is in general not unique. In fact, there may be infinitely many different factorizations, and it is not hard to see why. Consider for example the operator $L = D^2 \in C(x)[D]$. Every polynomial $\alpha + x \in C[x]$ is annihilated by D^2, and since $\alpha + x$ is also annihilated by $D - \frac{1}{\alpha+x}$, the operator $\operatorname{gcrd}(D^2, D - \frac{1}{\alpha+x}) = D - \frac{1}{\alpha+x}$ must be a nontrivial right factor of D^2, for every choice $\alpha \in C$. Another factorization is of course $L = DD$.

Although this example seems to indicate the opposite, it turns out that the factorization of an operator is essentially unique. In order to see in which sense, we will view the factorization of operators as structural properties of modules. For a given operator $L \in K[\partial]$, consider the module $K[\partial]/\langle L\rangle$. If L admits a nontrivial factorization $L = AB$, then the equivalence class $[B]$ generates a nontrivial submodule of $K[\partial]/\langle L\rangle$: it is the K-vector space generated by $[B], [\partial B], \dots, [\partial^{\operatorname{ord}(A)-1} B]$. Conversely, suppose that $K[\partial]/\langle L\rangle$ has a nontrivial submodule (i.e., a submodule other than $\{0\}$ and $K[\partial]/\langle L\rangle$), and let $B \in K[\partial]$ be such that $[B]$ is one of its elements. Then $[B], [\partial B], \dots$ generate a K-subspace of $K[\partial]/\langle L\rangle$ of dimension less than $\operatorname{ord}(L)$, say of dimension s. This means that the elements $[B], \dots, [\partial^s B]$ of $K[\partial]/\langle L\rangle$ are linearly dependent over K, so there is an operator $A \in K[\partial]$ of order s with $A\cdot[B] = 0$. In other words, $\operatorname{rrem}(AB, L) = 0$, or $AB = QL$ for yet another operator $Q \in K[\partial]$. Because of $\operatorname{ord}(A) = s < \operatorname{ord}(L)$, we have $\operatorname{ord}\operatorname{lclm}(B, L) < \operatorname{ord}(B) + \operatorname{ord}(L)$, which by Exercise 13 of Sect. 4.2 implies that $\operatorname{ord}\gcd(B, L) > 0$, so L has a nontrivial right factor.

In summary, we have shown that $L \in K[\partial] \setminus K$ is irreducible if and only if the module $K[\partial]/\langle L\rangle$ is *simple*, meaning its only submodules are $\{0\}$ and $K[\partial]/\langle L\rangle$. Finding a right factor of $L \in K[\partial] \setminus K$ is therefore equivalent to finding a nontrivial submodule of $K[\partial]/\langle L\rangle$. More generally, a factorization of L into k irreducible factors translates into a chain of submodules

$$\{0\} =: M_0 \subsetneq \cdots \subsetneq M_k := K[\partial]/\langle L\rangle$$

such that each of the quotient modules M_i/M_{i-1} $(i = 1, \ldots, k)$ is simple. The Jordan-Hölder theorem implies that if we have another chain

$$\{0\} =: N_0 \subsetneq \cdots \subsetneq N_\ell := K[\partial]/\langle L\rangle$$

with N_i/N_{i-1} simple $(i = 0, \ldots, \ell)$, then $k = \ell$ and there is a permutation $\pi : \{1, \ldots, k\} \to \{1, \ldots, k\}$ such that $M_i/M_{i-1} \cong N_{\pi(i)}/N_{\pi(i)-1}$ for $i = 1, \ldots, k$. In this sense, the factorization of an operator is unique.

Example 4.49

1. The operator $L = D^2 \in C(x)[D]$ admits, among others, two factorizations $L = DD$ and $L = (D + \frac{1}{x-1})(D - \frac{1}{x-1})$. Let M_1, N_1 be the submodules of $C(x)[D]/\langle L\rangle$ generated by $[D]$ and $[D - \frac{1}{x-1}]$, respectively. We then have

$$0 \subsetneq M_1 \subsetneq C(x)[D]/\langle L\rangle \quad \text{and} \quad 0 \subsetneq N_1 \subsetneq C(x)[D]/\langle L\rangle.$$

   Moreover, according to the discussion above, we should have $M_1 \cong N_1$ and

$$(C(x)[D]/\langle L\rangle)/M_1 \cong (C(x)[D]/\langle L\rangle)/N_1.$$

   Indeed, it can be checked (Exercise 3) that automorphisms are given by

$$M_1 \to N_1 \quad [qD] \mapsto [(x-1)qD - q],$$
$$(C(x)[D]/\langle L\rangle)/M_1 \to (C(x)[D]/\langle L\rangle)/N_1 \quad [q] \mapsto [\frac{1}{x-1}q],$$

   for $q \in C(x)$.
2. The operator $L = S^2 - x \in C(x)[S]$ is irreducible, because if it were reducible, it would have a right factor of order 1, and the algorithms of Sect. 2.6 can be used to check that this is not the case. It follows that $C(x)[S]/\langle S^2 - x\rangle$ has no nontrivial submodules, i.e., none of the one-dimensional $C(x)$-subspaces of $C(x)[S]/\langle S^2 - x\rangle$ are closed under application of S. □

In the commutative case, we have the relation $pq = \operatorname{lcm}(p, q)\gcd(p, q)$ for any two monic polynomials $p, q \in C[x]$. Since two distinct monic irreducible polynomials $p, q \in C[x]$ cannot have a common factor, we have $pq = \operatorname{lcm}(p, q)$ for such polynomials. The situation in the noncommutative case is different. Here, we must distinguish the question of whether an operator $L = K[\partial]$ can be written as the product of two smaller operators from the question of whether we can write it as the least common left multiple of two smaller operators. Of course, the latter implies the former, since $L = \operatorname{lclm}(A_1, A_2)$ implies the existence of B_1, B_2 such that $L = B_1 A_1 = B_2 A_2$. The converse, however, is not true.

Example 4.50 The operator $L = (xD + 1)D \in C(x)[D]$ is evidently the product of two first order operators. However, it cannot be written as a least common left multiple of two first order operators. To see why, note that $\log(x)$ is a solution of L. If we had $L = \operatorname{lclm}(D - a, D - b)$ for some $a, b \in C(x)$, then L would have two C-linearly independent hyperexponential solutions. In a differential field containing these solutions as well as $\log(x)$, there would be three linearly independent solutions, which by Theorem 3.20 is impossible if $\operatorname{ord}(L) = 2$. □

For a given operator, we can ask whether it can be written as a least common left multiple of smaller operators. As we have seen in the example above, this may not be the case even if the operator is not irreducible. If it is the case that the operator can be broken into a least common left multiple of one or more irreducible operators, we call it completely reducible.

Definition 4.51 An operator $L \in K[\partial] \setminus \{0\}$ is called *completely reducible* if there are irreducible operators $P_1, \ldots, P_k \in K[\partial]$ such that $L = \operatorname{lc}(L) \operatorname{lclm}(P_1, \ldots, P_k)$. □

Note that the case $k = 1$ is not excluded, so that the terminology as introduced in Definition 4.51 has the somewhat odd-looking side effect that every operator which is irreducible in the sense of Definition 4.48 is completely reducible in the sense of Definition 4.51. In the language of modules, we have seen above that L is irreducible if and only if $K[\partial]/\langle L\rangle$ is a simple module, i.e., one that has no submodules other than $\{0\}$ and $K[\partial]/\langle L\rangle$. Complete reducibility of an operator also translates into a classical notion of module theory: L is completely reducible if and only if $K[\partial]/\langle L\rangle$ is semisimple. A module M is called semisimple if it is a direct sum of simple submodules, or, equivalently, if for every submodule U of M there is another submodule W of M such that $M = U \oplus W$. The connection is established in the following proposition.

Proposition 4.52 *$L \in K[\partial] \setminus K$ is completely reducible if and only if $K[\partial]/\langle L\rangle$ is semisimple.* □

Proof "$\Rightarrow$": Let $L = \operatorname{lclm}(P_1, \ldots, P_k)$ for some monic and pairwise distinct irreducible operators $P_1, \ldots, P_k \in K[\partial]$. We can assume that the set of these operators is chosen minimally in the sense that no P_i is a right divisor of $\operatorname{lclm}(P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k)$. Since the P_i are irreducible, we then have $\operatorname{ord}(L) = \operatorname{ord}(P_1) + \cdots + \operatorname{ord}(P_k)$.

Consider the natural module homomorphism

$$h\colon K[\partial]/\langle L\rangle \to K[\partial]/\langle P_1\rangle \times \cdots \times K[\partial]/\langle P_k\rangle.$$

Because $\langle L\rangle = \langle P_1\rangle \cap \cdots \cap \langle P_k\rangle$, the map h is injective. Since h is also a K-linear map between two K-vector spaces of the same dimension, it is even an isomorphism. We therefore have

$$K[\partial]/\langle L\rangle = h^{-1}(K[\partial]/\langle P_1\rangle \times \{0\}^{k-1}) \oplus \cdots \oplus h^{-1}(\{0\}^{k-1} \times K[\partial]/\langle P_k\rangle).$$

Since the P_i are irreducible, the $K[\partial]/\langle P_i\rangle$ are simple, and since h is an isomorphism, their preimages are simple as well. We have therefore written $K[\partial]/\langle L\rangle$ as a direct sum of simple submodules, so $K[\partial]/\langle L\rangle$ is semisimple.

"$\Leftarrow$": For every submodule M of $K[\partial]/\langle L\rangle$ there is a $Q \in K[\partial] \setminus \{0\}$ of minimal order such that M is generated by $[Q]$ (Exercise 10). It is then generated as a K-vector space by $[Q], \dots, [\partial^{\operatorname{ord}(L)-\operatorname{ord}(Q)-1}Q]$, and the linear dependence of $[Q], \dots, [\partial^{\operatorname{ord}(L)-\operatorname{ord}(Q)}Q] \in K[\partial]/\langle L\rangle$ over K shows that there is a $P \in K[\partial]$ with $\operatorname{ord}(P) = \operatorname{ord}(L) - \operatorname{ord}(Q)$ such that $PQ = L$. This implies that $M \cong K[\partial]/\langle P\rangle$, and if M is simple, P is irreducible.

Suppose that $M_1, \dots, M_k \subseteq K[\partial]/\langle L\rangle$ are simple submodules such that

$$K[\partial]/\langle L\rangle = M_1 \oplus \cdots \oplus M_k,$$

and let $P_1, \dots, P_k$ be irreducible such that $M_i \cong K[\partial]/\langle P_i\rangle$ for $i = 1, \dots, m$. Writing $[1] = m_1 + \cdots + m_k$ with $m_1 \in M_1, \dots, m_k \in M_k$ shows that $\operatorname{lclm}(P_1, \dots, P_k)$ annihilates $[1]$ and is thus a left multiple of L. Since $\operatorname{ord}(P_i) = \dim_K(M_i)$ for $i = 1, \dots, k$ and $\operatorname{ord}(L) = \dim_K K[\partial]/\langle L\rangle = \dim_K(M_1) + \cdots + \dim_K(M_k)$, the order of $\operatorname{lclm}(P_1, \dots, P_k)$ cannot exceed $\operatorname{ord}(L)$. We must therefore have $L = \operatorname{lc}(L)\operatorname{lclm}(P_1, \dots, P_k)$, as claimed. ■

So far, we have only discussed general properties of factorization in $K[\partial]$ but no algorithms for finding factors. In Sect. 1.4, we have remarked that there is no general factorization algorithm for the commutative ring $C[x]$ of univariate polynomials over a field C. Instead, the ground field C determines if and how we can factor polynomials. As the commutative case is a special case of the factorization problem in an Ore algebra $K[\partial]$, it is clear that we can also not expect a uniform factorization algorithm applicable to all Ore algebras. We must make certain assumptions on $K[\partial]$, some of which will be "with loss of generality".

Without loss of generality, it suffices to focus on right factors. The reason is that if $K[\partial]$ is an Ore algebra with certain maps $\sigma, \delta\colon K \to K$, we can associate to it the Ore algebra $K[\partial^*]$ with $\sigma^*\colon K \to K$ defined by $\sigma^* = \sigma^{-1}$ and $\delta^*\colon K \to K$ defined by $\delta^* = -\delta \circ \sigma^{-1}$. For every $P = p_0 + p_1\partial + \cdots + p_r\partial^r \in K[\partial]$ we can then define $P^* = p_0 + \partial^* p_1 + \cdots + (\partial^*)^r p_r \in K[\partial^*]$. The operator $P^* \in K[\partial^*]$ is called the *adjoint* of $P \in K[\partial]$. A key feature of the adjoint is that $(PQ)^* = Q^*P^*$, so it translates right factors to left factors and vice versa.

It is also without loss of generality that we can restrict our attention to Ore algebras with $\sigma = \mathrm{id}$ or $\delta = 0$. The reason is that if $K[\partial]$ is an Ore algebra with certain maps $\sigma, \delta\colon K \to K$ with $\sigma \neq \mathrm{id}$, it is isomorphic to the Ore algebra $K[\tilde{\partial}]$ with σ and 0. As shown in Exercise 14, any choice $\alpha \in K$ with $\sigma(\alpha) \neq \alpha$ gives rise to an isomorphism $h\colon K[\tilde{\partial}] \to K[\partial]$ defined by

$$h(\tilde{\partial}) = \alpha\partial - \partial\alpha.$$

This operation is known as the *Hilbert twist.*

For an Ore algebra $K[\partial]$ with $\sigma = \mathrm{id}$ or $\delta = 0$, let $\theta\colon K \to K$ be equal to σ if $\sigma \neq \mathrm{id}$, and equal to δ otherwise. We will make the following assumptions throughout the rest of this section:

Assumption 4.53

1. $\sigma = \mathrm{id}$ or $\delta = 0$.
2. C is an algebraically closed field and for every $p \in C[x]$ with $\deg p > 0$ we can compute a root.
3. There is an algorithm which for given $p_0, \ldots, p_r \in K$, $p_r \neq 0$, computes a basis of the C-vector space of all $y \in K$ with $p_0 y + p_1\theta(y) + \cdots + p_r\theta^r(y) = 0$.
4. For any $L \in K[\partial]$ there is a module F such that L admits a solution space $V(L)$ in F with $\dim_C V(L) = \mathrm{ord}(L)$ and no operator has a solution space whose dimension exceeds its order.

The first assumption is justified by the Hilbert twist. The second assumption saves us from the trouble related to factorization in $C[x]$ which technically is included as a special case, but which is not really our business here. The third assumption is justified at least in the cases $C(x)[S]$ and $C(x)[D]$, by the techniques discussed in Sects. 2.5 and 3.5. The fourth assumption can also be justified for these algebras, using the Picard-Vessiot theory briefly sketched at the ends of Sects. 2.2 and 3.2. Note that the assumption is only that an appropriate module F exists, not that we can actually construct it or compute the solutions it is supposed to contain.

We first describe an algorithm which is relatively easy but is only guaranteed to succeed for completely reducible operators. This algorithm is known as the eigenring method. Let $L \in K[\partial]$ and $r = \mathrm{ord}(L)$. The idea of the eigenring method is to search for operators $P \in K[\partial]$ which commute with ∂ modulo L in the sense that we have $[P\partial] = [\partial P]$ in $K[\partial]/\langle L\rangle$. The commutation with ∂ ensures that any such operator P acts as a C-linear map on the solution space $V(L)$. Eigenvectors of this C-linear map are elements of $V(L)$ on which P acts like a multiplication by a constant λ, the corresponding eigenvalue. This means that $P - \lambda$ annihilates the eigenvectors, so these eigenvectors are common solutions of $P - \lambda$ and L and hence of $\mathrm{gcrd}(P - \lambda, L)$. If we arrange that $0 < \mathrm{ord}(P) < \mathrm{ord}(L)$, then this greatest common right divisor will be a nontrivial right factor of L.

An operator P which commutes with ∂ modulo L amounts to a C-linear map from $V(L)$ to itself. It is clear that every element of the class $[P] \in K[\partial]/\langle L\rangle$ amounts to the same map. In particular, P commutes with ∂ modulo L if and only if $\mathrm{rrem}(P, L)$ commutes with ∂ modulo L. Moreoever, the set of all operators P which commute with ∂ modulo L is closed under addition and multiplication (Exercise 12) and therefore forms a subring of $K[\partial]$. Then the subset of $K[\partial]/\langle L\rangle$ consisting of all classes $[P]$ with $[P\partial] = [\partial P]$ also forms a ring together with the operations $[P] + [Q] := [P + Q]$ and $[P][Q] := [PQ]$. This ring is called the *eigenring* of L and denoted by E_L.

Since an operator P which commutes with ∂ modulo L maps solutions of L to solutions of L, we must have $\operatorname{rrem}(LP, L) = 0$ for any such P. Conversely, if P is such that $\operatorname{rrem}(LP, L) = 0$, then LP annihilates all elements of $V(L)$, so P maps solutions of L to solutions of L. It is thus a C-linear map from $V(L)$ to itself and therefore commutes with ∂ modulo L. We have now shown that $[P]$ is an element of the eigenring of L if and only if $\operatorname{rrem}(LP, L) = 0$, and we can use the latter condition to find elements of the eigenring by making an ansatz $P = p_0 + p_1\partial + \cdots + p_{r-1}\partial^{r-1}$ with undetermined coefficients $p_0, \dots, p_{r-1} \in K$, computing $\operatorname{rrem}(LP, L)$ and equating the coefficients of powers of ∂ to zero. This leads to a coupled system of functional equations for the undetermined coefficients, whose solution space can be computed.

Once we have found an element $[P]$ of the eigenring, we have to find an eigenvalue of the corresponding linear map $V(L) \to V(L)$. This can be done in two ways. We can either construct the minimal polynomial of $[P]$ by finding a C-linear dependence between $[1], [P], [P^2], \dots$ and compute a root of this polynomial. Alternatively, we can exploit the fact that the resultant of two operators is zero if and only if the operators have a nontrivial greatest common right divisor (cf. Sect. 4.2). For an indeterminate z, the resultant $\operatorname{res}(L, P - z)$ is an element of $K[z]$ whose roots in C are exactly the eigenvalues of P.

Algorithm 4.54 *(Eigenring method)*
Input: $L \in K[\partial]$ *for an Ore algebra meeting the requirements specified in Assumption 4.53.*
Output: *A proper right factor of L, or an error message.*

1 *Compute a C-vector space basis* $\{[P_1], \dots, [P_d]\}$ *of the eigenring* E_L.
2 *If* $d = 1$, *return "failed".*
3 *Choose a basis element* $[P_i]$ *with* $0 < \operatorname{ord}(P_i) < \operatorname{ord}(L)$.
4 *Compute an eigenvalue* λ *of* $[P_i]$.
5 *Return* $\operatorname{gcrd}(L, P_i - \lambda)$.

Concerning lines 2 and 3, note that the eigenring always contains $[1]$, but that this element is not useful because its eigenvalue is 1, so we would only get $\operatorname{gcrd}(L, 0) = L$ in step 5. As soon as $d > 1$, there must be a basis element with $0 < \operatorname{ord}(P_i) < \operatorname{ord}(L)$.

Example 4.55

1. Consider $L = (x-1)D^2 - x^2D + (x^2 - x - 1) \in C(x)[D]$. For computing the eigenring, we make an ansatz $P = p_0 + p_1D$ and enforce $\operatorname{rrem}(LP, L) = 0$.

$$\operatorname{rrem}(LP, L) = \Big(-\frac{(x-2)xp_1}{x-1} - x^2p_0' - 2(1 - x + x^2)p_1' + (x-1)p_0''\Big)$$

$$+\Big(\frac{(x-2)xp_1}{x-1}+2(x-1)p_0'+x^2p_1'+(x-1)p_1''\Big)D,$$

and equating the coefficients of D^0 and D^1 to zero gives a system of two functional equations for the two unknowns p_0, p_1. This system has the two linearly independent solutions $(1,0)$ and $(-\frac{1}{x-1}, \frac{1}{x-1})$. They give rise to the basis $\{[1], [-\frac{1}{x-1}+\frac{1}{x-1}D]\}$ of the eigenring E_L. We choose $P=-\frac{1}{x-1}(1-D)$ and compute an eigenvalue. Since $\operatorname{rrem}(P^2, L)=P$, the minimal polynomial is $z^2-z=(z-1)z$, so the eigenvalues are 0 and 1. Either of them leads to a right factor of L:

$$\operatorname{gcrd}(L, P-0)=D-1, \quad \operatorname{gcrd}(L, P-1)=D-x.$$

In fact, we have $L=\operatorname{lclm}(D-1, D-x)$.

2. Consider $L=D^2-(x+1)D+(x-1)\in C(x)[D]$. In this case, the ansatz $P=p_0+p_1D$ leads to

$$\begin{aligned}\operatorname{rrem}(LP, L)&=(-p_1+(-1-x)p_0'-2(-1+x)p_1'+p_0'')\\&\quad+(p_1+2p_0'+(1+x)p_1'+p_1'')D,\end{aligned}$$

and equating the coefficients of D^0 and D^1 to zero gives a coupled system whose solution space turns out to be generated by $(p_0, p_1)=(1,0)$. Therefore, the algorithm aborts in line 2 with a failure. Note however that L admits the factorization $L=(D-1)(D-x)$. □

As long as no claim is made about the situations in which Algorithm 4.54 fails in finding a factor, it is obvious that the algorithm works as specified. Even an algorithm that trivially reports a failure for every input would be correct for this specification. The interesting feature of Algorithm 4.54 is that it is guaranteed to find a right factor whenever it is applied to an operator L which can be written as the least common left multiple of smaller operators.

Theorem 4.56 *Let $U, W \in K[\partial]$ be such that* $\operatorname{ord}(U), \operatorname{ord}(W) \geq 1$ *and* $\operatorname{grcd}(U, W)=1$. *Then Algorithm 4.54 applied to $L=$* $\operatorname{lclm}(U, W)$ *succeeds in finding a right factor.* □

Proof The algorithm only fails if the eigenring of L is generated by the class $[1]\in K[\partial]/\langle L\rangle$. (Keep in mind that we are assuming that C is algebraically closed, so there is no danger that there might not be any eigenvalue in line 4.) We show that this is not the case by exhibiting another element of the eigenring. By Theorem 4.21, there are $S, T\in K[\partial]$ such that $1=SU+TW$ and $\operatorname{ord}(S)<\operatorname{ord}(W)$, $\operatorname{ord}(T)<\operatorname{ord}(U)$. For $P=SU$ we have $0<\operatorname{ord}(P)<\operatorname{ord}(U)+\operatorname{ord}(W)=\operatorname{ord}(L)$. We show that $[P]$ is an element of the eigenring. Indeed, $\operatorname{rrem}(UP, U)=\operatorname{rrem}(USU, U)=0$ and $\operatorname{rrem}(WP, W)=\operatorname{rrem}(WSU, W)=\operatorname{rrem}(W(1-TW), W)=0$, so $LP=$

$\operatorname{lclm}(U, W)P$ contains both U and W as right factors. It therefore contains $L = \operatorname{lclm}(U, W)$ as a right factor, and we have shown $\operatorname{rrem}(LP, L) = 0$, as required. ■

As a corollary, if we know that L is completely reducible, then we can use Algorithm 4.54 to decide whether L is irreducible. This will be the case if and only if it fails to find a right factor. Algorithm 4.54 may also succeed with input that cannot be written as a least common left multiple. An example is the operator $(xD+1)D \in C(x)[D]$ from Example 4.50, for which it does find the right factor D although this operator is not a least common left multiple. In general, given an operator $L \in K[\partial]$ and a right factor U, it is not so obvious whether there is an operator $W \in K[\partial]$ with $\operatorname{gcrd}(U, W) = 1$ and $\operatorname{lclm}(U, W) = L$. If L is completely reducible, then the fact that $K[\partial]/\langle L\rangle$ is semisimple implies that for every right factor U of L there exists a suitable W. In general, it can happen that some right factors of L are part of an lclm and others are not. By the following theorem, whenever $L = AU$, then there exist B, W with $L = BW$ and $\operatorname{gcrd}(U, W) = 1$ if and only if there exists an S with $\operatorname{rrem}(US, A) = 1$. Testing this condition is similar to computing the eigenring.

Theorem 4.57

1. *If* $U, W, S, T, A, B \in K[\partial]$ *are such that* $SU + TW = 1$ *and* $AU - BW = 0$, *then* $\operatorname{rrem}(US, A) = 1$.
2. *If* $U, S, A \in K[\partial]$ *are monic and such that* $\operatorname{rrem}(US, A) = 1$, *and if* $W \in K[\partial]$ *is such that* $S \cdot y$ *is a solution of* W *if and only if* y *is a solution of* A, *then* $AU = \operatorname{lclm}(U, W)$. □

Proof

1. Let $L = AU = BW$. We consider the various operators as linear maps between solution spaces. The map $SU + TW = 1$ acts as identity on $V(L)$ and the map TW is the zero map on $V(W) \subseteq V(L)$, so SU is a projection of $V(L)$ onto $V(W)$ and acts as the identity on the image $V(W)$. The operator U maps $V(L)$ to $V(A)$ and has $V(U) \subseteq V(L)$ as the kernel. It is surjective because $\dim \operatorname{im} R = \dim V(L)/\ker R = \operatorname{ord}(L) - \operatorname{ord}(U) = \operatorname{ord}(A) = \dim V(A)$. Because of $SU + TW = 1$ we have $V(L) = V(U) \oplus V(W)$, hence U is an isomorphism from $V(W) \subseteq V(L)$ to $V(A)$. Since SU acts as the identity on $V(W)$, it follows that S is an isomorphism from $V(A)$ to $V(W)$. But then US acts as the identity on $V(A)$, so $US - 1$ maps $V(A)$ to zero, so $US - 1$ is a left multiple of A. It follows that $\operatorname{rrem}(US, A) = 1$.
2. If $\operatorname{rrem}(US, A) = 1$, then US acts on $V(A)$ as the identity, and S is an isomorphism from $V(A)$ to $S \cdot V(A)$. By assumption, $S \cdot V(A) = V(W)$. As US acts on $V(A)$ as the identity, U is an isomorphism from $V(W)$ to $V(A)$ and SU acts as the identity on $V(W)$. We therefore have $SU + TW = 1$ for a certain $T \in K[\partial]$, and hence $\operatorname{gcrd}(U, W) = 1$. It also follows that for every $y \in V(W)$ we have $U \cdot y \in V(A)$, i.e., $AU \cdot y = 0$. This means that W is a right factor of AU. Obviously, U is also a right factor of AU, so altogether $\operatorname{lclm}(U, W)$ is a right factor of AU. Since $V(W)$ and $V(A)$ are isomorphic,

we have $\operatorname{ord}(W) = \operatorname{ord}(A)$, and taking also $\operatorname{gcrd}(U, W) = 1$ into account, we have $\operatorname{ord}\operatorname{lclm}(U, W) = \operatorname{ord}(U) + \operatorname{ord}(W) = \operatorname{ord}(U) + \operatorname{ord}(A) = \operatorname{ord}(AU)$. Therefore, $\operatorname{lclm}(U, W) = pAU$ for some $p \in K$, but since A and U are monic by assumption, $p = 1$. ■

Unless we know that the input is completely reducible, the eigenring method cannot be used for deciding whether a given operator is irreducible or not. The algorithm explained next, which is known as Beke's algorithm, can solve the factorization problem completely. In addition to the assumptions on $K[\partial]$ imposed in Assumption 4.53, we now include the following further assumptions:

Assumption 4.58

1. There is an algorithm which for any given $L \in K[\partial]$ finds all of its first order right factors.
2. There is an algorithm for solving systems of polynomial equations in C.
3. If $\sigma = \mathrm{id}$, $\delta \neq 0$, then for every operator $L \in K[\partial]$ there is an extension field E of K with $\operatorname{Const}(E) = \operatorname{Const}(K)$ such that $V(L) \subseteq E$ has dimension $\operatorname{ord}(L)$.
4. If $\sigma \neq \mathrm{id}$, $\delta = 0$, then for every operator $L \in K[\partial]$ which is not a left multiple of ∂ there is an extension ring E of K like in Theorem 2.27, with $\operatorname{Const}(E) = \operatorname{Const}(K)$, and such that $V(L) \subseteq E$ has dimension $\operatorname{ord}(L)$.

The last two assumptions allow us to formulate Wronskians. Recall that we defined $\theta = \sigma$ if $\delta = 0$ and $\theta = \delta$ if $\sigma = \mathrm{id}$. The *Wronskian* of some elements $y_0, \ldots, y_{r-1} \in E$ is defined as the determinant

$$W(y_0, \ldots, y_{r-1}) := \begin{vmatrix} y_0 & y_1 & \cdots & y_{r-1} \\ \theta(y_0) & \theta(y_1) & \cdots & \theta(y_{r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{r-1}(y_0) & \theta^{r-1}(y_1) & \cdots & \theta^{r-1}(y_{r-1}) \end{vmatrix}.$$

Since θ is C-linear, it is clear that $W(y_0, \ldots, y_{r-1})$ is zero whenever $y_0, \ldots, y_{r-1}$ are C-linearly dependent. Conversely, if $y_0, \ldots, y_{r-1}$ are linearly independent over C and belong to the solution space $V(L) \subseteq E$ of some operator $L \in K[\partial]$, then $W(y_0, \ldots, y_{r-1})$ is nonzero. In this case, the Wronskian additionally satisfies a first order equation with coefficients in K. For differential equations, all of these facts are commonly covered in introductory courses, and the general assumptions declared above are chosen in such a way that the facts extend to the more general situation we consider here (Exercise 21).

Consider an operator $L = \ell_0 + \cdots + \ell_{r-1}\partial^{r-1} + \partial^r \in K[\partial]$ and let $y_0, \ldots, y_{r-1}$ be a basis of its solution space $V(L) \subseteq E$. If y is any element of $V(L)$, the elements $y, y_0, \ldots, y_{r-1}$ are linearly dependent, so their Wronskian is zero. Expanding the determinant along the first column, we get the equation

$$W_0 y - W_1\theta(y) \pm \cdots + (-1)^r W_r\theta^r(y) = 0,$$

with

$$W_i = \begin{vmatrix} y_0 & y_1 & \cdots & y_{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{i-1}(y_0) & \theta^{i-1}(y_1) & \cdots & \theta^{i-1}(y_{r-1}) \\ \theta^{i+1}(y_0) & \theta^{i+1}(y_1) & \cdots & \theta^{i+1}(y_{r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{r}(y_0) & \theta^{r-1}(y_1) & \cdots & \theta^{r}(y_{r-1}) \end{vmatrix} \qquad (i = 0, \dots, r).$$

Since W_r is the Wronskian, which is not zero, we can divide the equation by $(-1)^r W_r$ to obtain a monic operator in $E[\partial]$ of order r whose solution space is equal to $V(L)$. If this operator were different from L, its greatest common right divisor with L would be an operator of order less than r with an r-dimensional solution space. Since this is impossible, we must have $\ell_i = (-1)^{r-i} \frac{W_i}{W_r}$ for $i = 0, \dots, r-1$. In particular, the W_i are certain K-multiples of the Wronskian, and as such, they also satisfy certain first order equations.

If $L \in K[\partial]$ has a nontrivial right factor, then the coefficients of the right factor can also be expressed in terms of Wronskians. In particular, they satisfy certain first order equations. The key idea of the factorization algorithm is to generate from the input operator L some auxiliary equations which have these Wronskians as solutions. Since we assume that there is a way to find first order right factors, we can then determine candidates for the coefficients. Like in Sects. 2.6 and 3.6, these candidates will in general involve some undetermined constant parameters. By dividing L by such a parameterized candidate and forcing the remainder to zero, we finally get a system of polynomial equations for the parameters, which we can solve by assumption. The solutions give rise to the desired right factors.

It remains to be explained how to find suitable auxiliary equations. Suppose the input operator is $L = \ell_0 + \cdots + \ell_{r-1}\partial^{r-1} + \partial^r \in K[\partial]$, and let $s \in \{2, \dots, r-1\}$. We seek right factors of order s, i.e., a factorization

$$L = Q\,\underbrace{(p_0 + \cdots + p_{s-1}\partial^{s-1} + \partial^s)}_{:=P}$$

with $Q \in K[\partial]$ and $p_0, \dots, p_{s-1} \in K$. Let $y_0, \dots, y_{s-1}$ be a basis of $V(P)$ and $W_0, \dots, W_s \in E$ be the corresponding determinants as introduced above (with P playing the role of L). As determinants depend polynomially on their entries and the entries are defined in terms of L, we could use closure properties to construct for each of the determinants an annihilating operator. This would be a brutal approach. A somewhat less brutal way (but still quite costly) is to also exploit in the search that we need the $W_0, \dots, W_s \in E$ to be pairwise similar in the sense that $W_i/W_s \in K$ for all i. This can be done by considering the K-subspace of E generated by all $s \times s$ determinants

$$\begin{vmatrix} \theta^{i_1}(y_0) & \cdots & \theta^{i_1}(y_{s-1}) \\ \vdots & \ddots & \vdots \\ \theta^{i_s}(y_0) & \cdots & \theta^{i_s}(y_{s-1}) \end{vmatrix} \in E$$

with $0 \leq i_1 < \cdots < i_s < r$. There are $n := \binom{r}{s}$ many of these; let us call them Wronskian-type determinants and denote them by $\Delta_1, \ldots, \Delta_n$. Note that they include the determinants $W_0, \ldots, W_{s-1}$ we are interested in. It turns out that the K-vector space generated by $\Delta_1, \ldots, \Delta_n$ is closed under θ (Exercise 23), so there is a matrix $A \in K^{n\times n}$ with

$$\begin{pmatrix} \theta(\Delta_1) \\ \vdots \\ \theta(\Delta_n) \end{pmatrix} = A \begin{pmatrix} \Delta_1 \\ \vdots \\ \Delta_n \end{pmatrix}.$$

This matrix can be determined using only the input operator L, and the system can be solved using the techniques developed in the previous section.

Example 4.59

1. Consider $L = (x-1) + (x^2-1)S - xS^2 - (x-3)S^3 + S^4 \in C(x)[S]$. We want to decide if L has a right factor P of order $s = 2$. For a basis y_0, y_1 of $V(P)$, we consider the $\binom{4}{2} = 6$ determinants

$$\Delta_1 = \begin{vmatrix} y_0 & y_1 \\ \theta(y_0) & \theta(y_1) \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} y_0 & y_1 \\ \theta^2(y_0) & \theta^2(y_1) \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} y_0 & y_1 \\ \theta^3(y_0) & \theta^3(y_1) \end{vmatrix},$$

$$\Delta_4 = \begin{vmatrix} \theta(y_0) & \theta(y_1) \\ \theta^2(y_0) & \theta^2(y_1) \end{vmatrix}, \quad \Delta_5 = \begin{vmatrix} \theta(y_0) & \theta(y_1) \\ \theta^3(y_0) & \theta^3(y_1) \end{vmatrix}, \quad \Delta_6 = \begin{vmatrix} \theta^2(y_0) & \theta^2(y_1) \\ \theta^3(y_0) & \theta^3(y_1) \end{vmatrix}.$$

The potential factor P has the form $P = \frac{\Delta_4}{\Delta_1} - \frac{\Delta_2}{\Delta_1}S + S^2$. Since θ is an automorphism, it commutes with the determinant, so we get $\theta(\Delta_1) = \Delta_4$, $\theta(\Delta_2) = \Delta_5$, and $\theta(\Delta_4) = \Delta_6$ for free. For the remaining Δ_i, we first apply θ and then use $\theta^4(y_i) = (x+3)\theta^3(y_i) + x\theta^2(y_i) - (x^2-1)\theta(y_i) + (1-x)y_i$ to obtain $\theta(\Delta_3) = (x+3)\Delta_5 + x\Delta_4 - (1-x)\Delta_1$, $\theta(\Delta_5) = (x+3)\Delta_6 + (x^2-1)\Delta_4 - (1-x)\Delta_2$, $\theta(\Delta_6) = -x\Delta_6 + (x^2-1)\Delta_5 - (1-x)\Delta_3$. We can put these relations together into the system

$$\begin{pmatrix} \theta(\Delta_1) \\ \theta(\Delta_2) \\ \theta(\Delta_3) \\ \theta(\Delta_4) \\ \theta(\Delta_5) \\ \theta(\Delta_6) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1-x & 0 & 0 & x & x+3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1-x & 0 & x^2-1 & 0 & x+3 \\ 0 & 0 & 1-x & 0 & x^2-1 & -x \end{pmatrix} \begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \\ \Delta_4 \\ \Delta_5 \\ \Delta_6 \end{pmatrix}.$$

Up to constant multiples, this system has exactly one solution whose components $\Delta_1, \Delta_2, \Delta_4$ are pairwise similar hypergeometric terms. This solution is

$$(\Delta_1, \ldots, \Delta_6) = (-1)^x \, (1, x+1, x^2+3x+3, -1, -x-2, 1)$$

and gives rise to the candidate $P = \frac{\Delta_4}{\Delta_1} - \frac{\Delta_2}{\Delta_1} S + S^2 = -1 - (x+1)S + S^2$, which indeed is a right factor of L.

2. Now consider $L = S^4 - 2(x+1)S^3 + (x^2+x-2)S^2 + 2xS + 1 \in C(x)[S]$. With $\Delta_1, \ldots, \Delta_6$ defined as before, we now get the system

$$\begin{pmatrix} \theta(\Delta_1) \\ \theta(\Delta_2) \\ \theta(\Delta_3) \\ \theta(\Delta_4) \\ \theta(\Delta_5) \\ \theta(\Delta_6) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -x^2-x+2 & 2(x+1) & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2x & 0 & 2(x+1) \\ 0 & 0 & 1 & 0 & 2x & x^2+x-2 \end{pmatrix} \begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \\ \Delta_4 \\ \Delta_5 \\ \Delta_6 \end{pmatrix}.$$

In this case, the solutions with hypergeometric components form a three-dimensional vector space generated by

$$\begin{aligned} b_1 &= (-1)^x \, (0, -1, -2x, 0, 1, 0), \\ b_2 &= (-1)^x \, (1, x, x^2+x+1, -1, -x-1, 1), \\ b_3 &= (-1)^x \, (x, x^2, x^3+x^2+x+1, -x-1, -x^2-2x-1, x+2). \end{aligned}$$

These solutions give rise to the parameterized family

$$P = S^2 - \frac{c_3x^2 + xc_2 - c_1}{c_2 + c_3x} S - \frac{c_3x + c_3 + c_2}{c_2 + c_3x}$$

of candidates, where c_1, c_2, c_3 are undetermined elements of C. In order to find out which elements of the family really are right factors, we compute

$$\begin{aligned} \operatorname{rrem}(L, P) = {} & \frac{c_1^2 - c_2c_1 - c_3c_1 - c_3^2}{(c_3x + c_2)(c_3x + c_2 + 2c_3)} \\ & - \frac{(c_1^2 - c_2c_1 - c_3c_1 - c_3^2)(-c_3x^2 - c_2x + c_1)}{(c_3x + c_2)(c_3x + c_2 + c_3)(c_3x + c_2 + 2c_3)} S. \end{aligned}$$

Since P is a right factor of L if and only if this expression is zero, the right factors are those with $c_1^2 - c_2c_1 - c_3c_1 - c_3^2 = 0$ and $(c_2, c_3) \neq (0, 0)$. □

Beke's factorization algorithm can be summarized as follows.

Algorithm 4.60 *(Beke)*
Input: $L \in K[\partial] \setminus \{0\}$, $s \in \{2, \ldots, \operatorname{ord}(L) - 1\}$, *for an Ore algebra meeting the requirements of Assumptions 4.53 and 4.58.*
Output: *All right factors of L of order s.*

1 *Let* $n = \binom{\operatorname{ord}(L)}{s}$ *and write* $\Delta_1, \ldots, \Delta_n$ *for the* $s \times s$ *minors of the matrix* $((\theta^i(y_j)))_{i=0,j=0}^{r-1,s-1}$, *where* $y_0, \ldots, y_{s-1}$ *are place holders for some C-linearly independent solutions of L. Let* $i_0, \ldots, i_s \in \{1, \ldots, r\}$ *be the indices such that* Δ_{i_k} *is the minor obtained from the rows* $0, \ldots, k-1, k+1, \ldots, s$.
2 *Construct a matrix* $A \in K^{n \times n}$ *such that* $(\theta(\Delta_i))_{i=1}^n = A(\Delta_i)_{i=1}^n$.
3 *Find all solutions of the system from line 2 for which* $\Delta_{i_s} \neq 0$ *and the quotients* $\Delta_{i_j}/\Delta_{i_s}$ $(j = 0, \ldots, s)$ *are in K.*
4 *The result of line 3 is a finite union of finite dimensional C-vector spaces. For each of these spaces, do the following:*
5 *Let* $b_1, \ldots, b_d$ *be a basis and consider a generic element* $c_1 b_1 + \cdots + c_d b_d$ *with undetermined coefficients* $c_1, \ldots, c_d$.
6 *Make an ansatz* $P = \sum_{j=0}^{s} (-1)^j \frac{\Delta_{i_j}}{\Delta_{i_s}} \partial^j$ *with the* Δ_i*'s replaced by the respective component of the generic element from line 5.*
7 *Compute* $\operatorname{rrem}(L, P)$ *and compute all* $(c_1, \ldots, c_d) \in C^d$ *for which this remainder becomes zero. This may require solving a system of nonlinear equations. For every solution (or for an appropriate description of the solution set, if it is infinite), report the right factor P.*

Observe that in the computations for finding right factors, we never need to know any of the solutions $y_0, y_1, \ldots$ explicitly. All we really need is that they are solutions and that they are linearly independent over C. Instead of assuming certain particular solutions, we may as well do the computations with appropriate formal objects. Multilinear algebra offers such formal objects. Consider the module $M = K[\partial]/\langle L \rangle$ and recall that finding a right factor of L of order s is the same as finding a submodule N of M with $\dim_K(N) = s$. The *exterior power* $\bigwedge^s V$ of a K-vector space V is a construction similar to the tensor product. It consists of formal objects that are written $v_1 \wedge \cdots \wedge v_s$ with $v_1, \ldots, v_s \in V$, and of finite sums of such objects. Like the tensor product, these objects satisfy the rule

$$\begin{aligned} & v_1 \wedge \cdots \wedge v_{i-1} \wedge (p v_i + q v_i') \wedge v_{i+1} \wedge \cdots \wedge v_s \\ &= p\,(v_1 \wedge \cdots \wedge v_{i-1} \wedge v_i \wedge v_{i+1} \wedge \cdots \wedge v_s) \\ &+ q\,(v_1 \wedge \cdots \wedge v_{i-1} \wedge v_i' \wedge v_{i+1} \wedge \cdots \wedge v_s) \end{aligned}$$

for any $v_1, \ldots, v_s \in V$ and $p, q \in K$, and unlike tensor products, they satisfy the additional rule

$$v_1 \wedge \cdots \wedge v_s = \operatorname{sgn}(\pi)(v_{\pi(1)} \wedge \cdots \wedge v_{\pi(s)})$$

for any $v_1, \dots, v_s \in V$ and any permutation $\pi \in S_s$. If $b_1, \dots, b_r$ form a basis of V, then a basis of $\bigwedge^s V$ is given by the objects $b_{i_1} \wedge \cdots \wedge b_{i_s}$ for all choices $i_1, \dots, i_s \in \{1, \dots, r\}$ with $i_1 < \cdots < i_s$. In particular, $\dim_K \bigwedge^s V = \binom{\dim(V)}{s}$.

The axioms for the exterior power $\bigwedge^s V$ are chosen in such a way that for any $P_1, \dots, P_s \in K[\partial]$, the object $[P_1] \wedge \cdots \wedge [P_s] \in \bigwedge^s K[\partial]/\langle L\rangle$ can be interpreted as a determinant

$$\begin{vmatrix} P_1 \cdot y_1 & \cdots & P_1 \cdot y_s \\ \vdots & \ddots & \vdots \\ P_s \cdot y_1 & \cdots & P_s \cdot y_s \end{vmatrix}$$

where $y_1, \dots, y_s$ are C-linearly independent solutions of L in some extension E of K. In accordance with this interpretation, we turn the K-vector space $\bigwedge^s K[\partial]/\langle L\rangle$ into a $K[\partial]$-module. Depending on whether $\theta = \sigma$ or $\theta = \delta$, the action of ∂ is defined through

$$\delta(v_1 \wedge \cdots \wedge v_s) = \sum_{i=1}^{s} (v_1 \wedge \cdots \wedge v_{i-1} \wedge \delta(v_i) \wedge v_{i+1} \wedge \cdots \wedge v_s),$$

$$\text{or } \sigma(v_1 \wedge \cdots \wedge v_s) = \sigma(v_1) \wedge \cdots \wedge \sigma(v_s).$$

Then $\bigwedge^s K[\partial]/\langle L\rangle$ corresponds to the K-vector space generated by all Wronskian-type determinants considered in Beke's algorithm, and the module structure imposed on it reflects the fact that this space is closed under applying θ.

It can be checked that whenever N is a submodule of $K[\partial]/\langle L\rangle$ with $\dim_K N = s$, then $\bigwedge^s N$ is (isomorphic to) a submodule of $\bigwedge^s K[\partial]/\langle L\rangle$. Since $\dim_K(\bigwedge^s N) = \binom{s}{s} = 1$, we are interested in the one-dimensional submodules of $\bigwedge^s K[\partial]/\langle L\rangle$. The search for such submodules corresponds to the search for solution vectors with hyperexponential/hypergeometric components of the coupled system in Beke's algorithm. Not every one-dimensional submodule of $\bigwedge^s K[\partial]/\langle L\rangle$ must be of the form $\bigwedge^s N$ for some submodule N of $K[\partial]/\langle L\rangle$. The one-dimensional submodules of interest are those which are generated by an element of the form $v_1 \wedge \cdots \wedge v_s$ (rather than by a certain K-linear combination of such terms). Searching within the set of all one-dimensional submodules for those of the required form corresponds to line 7 in Beke's algorithm where we compute the right remainder of L by a generic element involving parameters and solve a system of nonlinear equations in order to force the remainder to zero.

In conclusion, we do not lose anything by considering exterior powers instead of Wronskian-type determinants. We can however gain something by importing some general knowledge about exterior powers. In particular, the so-called Plücker relations can be used to substantially reduce the computational complexity of the algorithm. We do not discuss this here but refer to the literature for this optimization and other improvements.

Even when all known optimizations are applied, factorization of operators is extremely expensive. We have seen in Sects. 2.6 and 3.6 that finding hypergeometric and hyperexponential solutions involves a combinatorial search which may take an exponential amount of time. Here we apply these algorithms to operators of order $\binom{r}{s}$, and this binomial is itself exponential when r grows and r/s is approximately constant. In practice, this can mean that checking whether an operator of order 10 is irreducible might well be infeasible.

In order to show that a given operator of order r is irreducible, we can apply Beke's algorithm to search for right factors of order s, for any $s < r$. It is irreducible if and only if this search yields no results. In order to write a given operator of order r as a product of irreducible operators, we can use Beke's algorithm to find some right factor and then apply it recursively to factor the factors. To keep the growth of $\binom{r}{s}$ under control, it is a good idea to start with small factors, and to also exploit that finding a right factor of order s is the same as finding a left factor of order $r - s$. An implementation will roughly look as follows.

Algorithm 4.61
Input: $L \in K[\partial] \setminus \{0\}$ *satisfying Assumptions* 4.53 *and* 4.58.
Output: *A list* $(P_1, \dots, P_m)$ *of irreducible elements of* $K[\partial]$ *such that* $L = P_1 \cdots P_m$.

if $\operatorname{ord}(L) = 1$ *then*
    Return (L).
Use the eigenring method (Algorithm 4.54*) to search for a right factor* P*. If it succeeds, apply the algorithm recursively to* $\operatorname{rquo}(L, P)$ *as well as to* P*, and return the concatenation of the resulting lists. Otherwise, continue as follows.*
for $s = 1, \dots, \lfloor \operatorname{ord}(L)/2 \rfloor$ *do*
    Search for a right factor P *of* L *of order* s.
    if there is one then
        Recursively compute a factorization $(P_1, \dots, P_{m-1})$ *of the right quotient* $\operatorname{rquo}(L, P)$ *and return* $(P_1, \dots, P_{m-1}, P)$.
    else if $s \neq \operatorname{ord}(L)/2$ *then*
        Using the adjoint, search for a left factor P *of* L *of order* s.
        if there is one then
            Recursively compute a factorization $(P_2, \dots, P_m)$ *of the left quotient* $\operatorname{lquo}(L, P)$.
            Return $(P, P_2, \dots, P_m)$.
Return (P).

One reason why factorization of operators is more difficult than factorization in commutative polynomial rings $C[x]$ is that the solution set of an operator is a C-vector space while the roots of a polynomial $p \in C[x]$ are only finitely many. Since every root of $p \in C[x]$ must be a root of one of its factors, it is possible to design factorization algorithms for $C[x]$ based on the idea of approximating a root (for instance numerically) and then constructing a polynomial q of degree less than

$\deg(p)$ that has, up to the approximation error, the same root. Then $\gcd(p, q)$ is a factor of p, and by making the approximation accuracy sufficiently high and the coefficients of q sufficiently small (in a suitable measure), it can be ensured that $\gcd(p, q) = 1$ implies that p is irreducible.

For an operator L, say in the differential case, we can also select a solution, say in $C[[x]]$, compute it to a high accuracy, then use guessing (Sect. 1.5) to find a candidate for a lower order annihilating operator P of the solution, and, if we find one, compute $\operatorname{gcrd}(P, L)$ to obtain a right factor of L. The problem is that it is not obvious how to select the solution in the first place. The solutions that are annihilated by a right factor of L belong to a subspace of $V(L)$, and if we take an arbitrary element of $V(L)$, it is very unlikely that this element belongs to such a subspace.

We can increase our chances a bit by considering generalized series solutions at a singularity rather than power series solutions at an ordinary point. Suppose that $L = \operatorname{lclm}(P, Q)$ for some P, Q and assume that ξ is a non-apparent singularity of P but not of Q. Then every generalized series solution of Q at ξ is in fact a power series, but P must have at least one generalized series solution at ξ which is not a power series. Since the solutions of P are also solutions of L, we can take one of the generalized series solutions of L at ξ which is not a power series and use guessing to find an annihilating operator of order less than $\operatorname{ord}(L)$ for it. If we take sufficiently many terms of the generalized series into account, this computation is guaranteed to find an operator which has a nontrivial greatest common right divisor with L. Similarly, if $L = QP$ and there is a singularity ξ at which there are generalized series solutions with more than $\operatorname{ord}(Q)$ many different types, then there must be one type for which all generalized series solutions of L are already annihilated by P, because Q cannot have more than $\operatorname{ord}(Q)$ many linearly independent solutions.

Example 4.62 The operator

$$\begin{aligned} L = 36x^2D^4 + 144xD^3 + (36x^3 - 36x^2 + 9x + 80)D^2 \\ + 18D + (x-1)(9x+8) \in C(x)[D] \end{aligned}$$

has no first order right factors, and we want to know if there are any second order factors. The indicial polynomial of L at $\xi = 0$ is $\eta = 4x(x-1)(3x-2)(3x-1)$, its roots $0, 1/3, 2/3, 1$ belong to three different $\mathbb{Z}$-equivalence classes. Therefore, if there is a factorization $L = QP$ with $\operatorname{ord}(Q) = \operatorname{ord}(P) = 2$, then for at least one of these classes, all of its corresponding generalized series solutions must be annihilated by P. For the exponent $1/3$, the only generalized series solution (up to constant multiples) is

$$x^{1/3}(1 - \tfrac{3}{8}x + \tfrac{9}{320}x^2 - \tfrac{9}{10240}x^3 + \tfrac{27}{1802240}x^4 + \cdots).$$

With a few more terms, guessing can find the candidate annihilating operator $P = 36x^2D^2 + (9x + 8)$, and we can easily check that P is indeed a right factor of L by computing $\operatorname{rrem}(L, P) = 0$. On the other hand, for the exponent 1, we have the solution

$$x^1(1 - \tfrac{9}{80}x + \tfrac{563}{53760}x^2 - \tfrac{40907}{23654400}x^3 + \tfrac{1945123}{17220403200}x^4 + \cdots),$$

and even with hundreds of additional terms, we do not find any plausible candidates for annihilating operators of order 2. □

Exercises

1. Fix a $c \in C$ and let $L = (S - c)^2 \in C(x)[S]$. Determine all first order right factors of L.

2. The minimal polynomial of an algebraic function or algebraic number is always irreducible. Is it also true that the minimal order annihilating operator of a D-finite function is always irreducible?

3*. Check that the maps in Example 4.49 are indeed module isomorphisms.

4*. Let $L \in K[\partial]$ and $r = \operatorname{ord}(L)$. Show that L is irreducible if and only if every nonzero vector $p \in K^r$ is cyclic for the companion matrix C_L.
Hint: Use the isomorphism of Exercise 16 of Sect. 4.3.

5. Find an operator $L \in C(x)[S]$ which is reducible but not completely reducible.

6. Let K be a differential field and $L \in K[D]$. Let E be an extension of K such that $V(L) \subseteq E$ has dimension $\operatorname{ord}(L)$. Show that L is completely reducible when viewed as an element of $E[D]$.

7. Let M be a $K[\partial]$-module and consider a chain of submodules $\{0\} = M_0 \subsetneq \cdots \subsetneq M_k = M$ such that M_i/M_{i-1} is simple for every $i = 1, \dots, k$. Prove or disprove: For every permutation $\pi \in S_k$ there exists a chain of submodules $\{0\} = N_0 \subsetneq \cdots \subsetneq N_k = M$ such that N_i/N_{i-1} is simple for every $i = 1, \dots, k$ and $N_{\pi(i)} \cong M_i$ for every $i = 1, \dots, k$.

8*. Prove or disprove:
a. If $L_1, L_2 \in K[\partial]$ are irreducible, then so is $L_1 \otimes L_2$.
b. If $P_1, P_2, P_3 \in K[\partial]$ are monic, irreducible, and pairwise distinct, then P_3 cannot be a right factor of $\operatorname{lclm}(P_1, P_2)$.
c. If $L \in C(x)[D]$ is completely reducible, then every formal power series solution of L is a C-linear combination of certain formal power series solutions of the right factors of L.

9. Show that $L \in C[\partial]$ is completely reducible if and only if it is squarefree.

10. Show that for every $M \subseteq K[\partial]/\langle L\rangle$ there is a $P \in K[\partial]$ such that M is generated by $[P]$.

11*. Write $C(x)[S]/\langle \operatorname{lclm}(S - x, S - x^2)\rangle$ as a direct sum of two submodules.

12****.** Show that the eigenring of an operator is indeed a ring.

13. (Manfred Buchacher) Show that if L is completely reducible and U is a right divisor of L, then U is completely reducible.

14***.** Check that the Hilbert twist is an algebra isomorphism and that it turns δ into zero.

15***.** Show that $(PQ)^* = Q^* P^*$ and $P^{**} = P$ for all $P, Q \in K[\partial]$.

16****.** Show that an irreducible operator $P \in C(x)[D]$ has either only algebraic solutions or only transcendental solutions (except 0).

Hint: First show that every algebraic function has an annihilating operator in $C(x)[D]$ which only has algebraic solutions.

17. Show that $\operatorname{gcld}(A, B) = \operatorname{gcrd}(A^*, B^*)^*$ for all $A, B \in K[\partial]$. Here, gcld refers to the greatest common left divisor, whose definition is analogous to Definition 4.19.

18. In the case $\sigma \neq \mathrm{id}$, $\delta = 0$, show that every factorization of a monic operator $L \in K[\partial]$ with $\operatorname{rrem}(L, \partial) = 0$ into irreducible factors contains one factor ∂. Show also that the corresponding statement is false in the case $\sigma = \mathrm{id}$, $\delta \neq 0$.

19. In the proof of Theorem 4.56 we used the fact that whenever $L = AU = BV$ for some operators $L, A, U, B, V \in K[\partial]$, then $\operatorname{lclm}(U, V)$ is a right divisor of L. Why is this true?

20. Write the following operators as least common left multiples:

a. $(1 - x^3)D^5 + 3x^2 D^4 + (x^4 - 7x)D^3 + 3D^2 + (2x^5 - 2x^2)D + 2x^4 - 8x$;

b. $(x^3 - 3x - 2)D^4 + (-x^4 + x^3 - x + 1)D^3 + (-2x^4 + 2x^3 + 3x^2 + 4x - 1)D^2 + (x^5 - 2x^2 + 3x)D - x^4 + 2x - 3$;

c. $(x^3 + x^2 - 4x - 4)S^4 + (-x^4 - 2x^3 + 3x^2 + 3x - 1)S^3 + (-2x^4 - 5x^3 + 8x^2 + 20x + 5)S^2 + (x^5 + 4x^4 + 2x^3 - 5x^2 - 9x - 9)S - x^4 - 4x^3 - x^2 + 6x$;

d. $S^4 - S^2 + (2x + 3)S - x^2 - 2x$.

21***.** Let $L = \partial^r - \ell_{r-1}\partial^{r-1} - \cdots - \ell_0 \in K[\partial]$ and let $y_0, \ldots, y_{r-1} \in E$ be a set of solutions.

a. Assuming $\sigma \neq \mathrm{id}$, $\delta = 0$, show that

$$\theta(W(y_0, \ldots, y_{r-1})) = \ell_0 W(y_0, \ldots, y_{r-1}).$$

b. Assuming $\sigma = \mathrm{id}$, $\delta \neq 0$, show that

$$\theta(W(y_0, \ldots, y_{r-1})) = \ell_{r-1} W(y_0, \ldots, y_{r-1}).$$

c. Show that $W(y_0, \ldots, y_{r-1})$ is nonzero whenever $y_0, \ldots, y_{r-1}$ are C-linearly independent.

22. Let $L \in C(x)[D]$, let g be an algebraic function, and let $M \in C(x)[D]$ be the minimal order operator such that for every solution f of L, the composition $f \circ g$ is a solution of M (cf. Theorem 3.29). Does irreducibility of L imply irreducibility of M?

23⋆. Show that the K-vector space generated by Δ_i is closed under θ.

24. Write the following operators as product of irreducible operators:

a. $D^4 - xD^3 + (2-x)D^2 + (x^2 - x - 5)D - x^2 + 4x + 1$;

b. $D^5 + D^4 - xD^3 + (x-4)D^2 + (2x-1)D - x^2 + x + 1$;

c. $S^4 - 3S^2 + (2x+1)S - x^2$;

d. $S^4 - xS^3 - xS^2 + (x^2-2)S - x^2 + 3x$.

25. Determine all second order right factors of $D^5 - D^3 \in C(x)[D]$.

26. In Algorithm 4.61, we assume that the subroutine for finding right factors just delivers one factor, but we have seen that we may find a parameterized family of factors in one stroke. How can Algorithm 4.61 be modified so as to take advantage of such a situation?

27. In view of $\binom{r}{s} = \binom{r}{r-s}$, what is the point of using adjoints in Algorithm 4.61 for finding left factors?

28. (Maximilian Jaroschek) Let $L \in K[\partial]$ and suppose there is a $P \in K[\partial]$ and a $k \in \mathbb{N}$ such that $L = P^k$.

a. In the case $\sigma = \mathrm{id}$, show that there exists a $p \in K$ with $p = \mathrm{lc}(P)^k$.

b. In the case $\delta = 0$, show that there exists a $p \in K$ with $p = ([\partial^0]P)^k$.

29⋆. In this section, we have discussed the factorization problem for Ore algebras $K[\partial]$ over a field K. The factorization problem also makes sense in Ore algebras $R[\partial]$ where R is just a ring, for example in $C[x][D]$. Show that $L = (4x-4)D^2 + (6x-4)D - 9$ is irreducible as element of $C[x][D]$ but not as element of $C(x)[D]$.

30⋆. In this section, we have discussed the factorization problem with respect to the multiplication of an Ore algebra. Alternatively, we could also consider the factorization problem with respect to the symmetric product, i.e., we could ask whether a given operator $L \in K[\partial]$ can be written as the symmetric product of some operators of lower order. Show that the operator $L = D^4 - 6D^3 + 11D^2 - 6D \in C(x)[D]$ can be factored in this sense.

References

The Jordan-Hölder theorem is more widely known for groups, a proof for its module version can be found in the book of Anderson and Fuller [31]. The connection between the Jordan-Hölder theorem and factorization of operators is nicely explained in a tutorial paper of Gomez-Torrecillas [219]. The discussion at the beginning of this section was inspired by this paper. A more direct proof of the essential uniqueness of a factorization is given in Ore's paper [344] (Thm. 1 in Chapter II). He also discusses complete reducibility (Sect. 2 of Chapter II), a concept that was first introduced by Loewy [315]. Loewy further showed that every operator can be written as a product of completely reducible operators. Such a factorization is called a Loewy decomposition. Loewy decompositions in the case of several variables were studied by Schwarz [400].

Giesbrecht [213, 214] introduced the eigenring method to factor elements of the Ore algebra $K[\partial]$ with $\delta = 0$ and K a finite field. In a sense, it is an adaption of Berlekamp's factorization algorithm for $\mathbb{Z}_p[x]$ [204] to the noncommutative setting. The approach was extended to arbitrary Ore algebras $C(t)[\partial]$ over a finite constant field C by Giesbrecht and Zhang [216]. Caruso and Le Borgne [123] propose a faster version of the algorithm. Singer [409] applies the eigenring method in characteristic zero for determining, without factoring, whether or not a differential operator is irreducible. At the end of this paper, Singer gives an account on the historical development of the ideas. Van Hoeij [442] proposes an efficient algorithm for finding elements of the eigenring.

The eigenring method is also sketched in Sect. 4.2.2 of the book by van der Put and Singer [441], and in some lecture notes of Li [310]. These two sources also discuss Beke's algorithm, and were a great help for preparing this section.

Beke's algorithm is due to Beke [52] and was first formulated for differential operators. It was improved by various people, including Schwarz [399], Grigoriev [226], Wolf [460], Bronstein [112], and Tsarev [429, 430]. For general Ore algebras, the algorithm was described by Bronstein and Petkovšek [115].

The idea to separate factors by analyzing local solutions at the singularities has been turned into a complete factorization algorithm by van Hoeij [443]. As this algorithm is more heavily based on the notion of solutions than the eigenring method or Beke's algorithm, it does not directly extend to other Ore algebras. Only very recently, some progress on an analogous algorithm for the shift case has been reported [475].

Another recent result which is useful for both theory and algorithm development is an explicit degree bound for the right factors a linear differential operator can have [98].

4.5 Several Variables

For an Ore algebra $K[\partial]$ acting on a module F, it is natural to think of ∂ as something like a derivation, and to view the elements of F as univariate objects with a variable on which the derivation acts. If there are several variables, we may want to use several derivations. For instance, we could associate one partial derivative to each variable. Definition 4.1 already offers this freedom, because it starts from an arbitrary ring R and declares what it means for $R[\partial]$ to be an Ore algebra. If R itself is already an Ore algebra, the construction yields an Ore algebra with two ∂'s, and if we want, we can iterate further to obtain an Ore algebra with as many ∂'s as we like. In this way we can construct, for example, an Ore algebra $C[x, y][\partial_1][\partial_2]$ which acts on the ring $C[[x, y]]$ of formal power series in two variables x, y, with ∂_1, ∂_2 acting as the partial derivations in x, y, respectively. We could also consider an Ore algebra $C[n,k][\partial_1][\partial_2]$ acting on the space $C^{\mathbb{N}\times\mathbb{N}}$ of sequences $((a_{n,k}))_{n,k=0}^{\infty}$ in two variables, with ∂_1, ∂_2 acting as shift operators with respect to n, k, respectively. It is also possible to construct Ore algebras with different types of operators, for instance letting ∂_1 be a derivation and ∂_2 be a shift operator gives an Ore algebra that acts on sequences of power series.

In general, two generators ∂_1, ∂_2 of an Ore algebra $R[\partial_1][\partial_2]$ need not commute. For example, if $R = C[x]$, $\sigma_1 = \mathrm{id}$, $\delta_1 = \frac{d}{dx}$, $\sigma_2(f(x)) = f(qx)$, $\delta_2 = 0$, where q is a nonzero constant, we have $\partial_1\partial_2 = q\partial_2\partial_1$. This situation is not typical, and by using the notation $R[\partial_1, \dots, \partial_n]$ instead of $R[\partial_1]\cdots[\partial_n]$, we shall indicate that the ∂_i do commute with each other. Although this commutativity is not a formal requirement of the theory, it represents the most relevant situation in applications, and we will mostly restrict our attention to this case. The arithmetic of such a *multivariate Ore algebra* $R[\partial_1, \dots, \partial_n]$ can be described by n endomorphisms $\sigma_1, \dots, \sigma_n \colon R \to R$ and n maps $\delta_1, \dots, \delta_n \colon R \to R$ such that δ_i is a σ_i-derivation for every i. We have the commutation rules $\partial_i\partial_j = \partial_j\partial_i$ and $\partial_i u = \sigma_i(u)\partial_i + \delta_i(u)$ for all $i, j = 1, \dots, n$.

For better readability, we will write $D_x, D_y, D_z, \dots$ for the elements of Ore algebras that behave like partial derivations with respect to $x, y, z, \dots$. We shall assume that these commute with each other (e.g., $D_xD_y = D_yD_x$) and that partial derivations commute with all of the variables they are not responsible for (e.g., $D_xy = yD_x$). Similarly, we will write $S_x, S_y, S_z, \dots$ for the shift operators that map $x, y, z, \dots$ to $x+1, y+1, z+1, \dots$, respectively. Also in this case, we have commutation rules like $S_xS_y = S_yS_x$ and $S_xy = yS_x$. Using this notation, the Ore algebras suggested above would be written as $C[x,y][D_x, D_y]$, $C[n,k][S_n, S_k]$, $C[x,n][D_x, S_n]$, respectively. Typically, we will consider Ore algebras $R[\partial_1, \dots, \partial_n]$ with $R = C[x_1, \dots, x_n]$ or $R = C(x_1, \dots, x_n)$ where each ∂_i commutes with every x_j ($i \neq j$). An example not matching this common pattern is the algebra $C(x)[D_x, S_x]$, in which we can shift as well as differentiate the variable.

In the univariate case, we have defined a function as D-finite if it has a nonzero annihilating operator. This definition is no longer useful in the multivariate setting. We use instead the criterion appearing in part 1 of Theorem 4.12 as a definition.

Definition 4.63 Let $A = K[\partial_1, \dots, \partial_n]$ be an Ore algebra over a field K and let F be an A-module.

1. For $f \in F$, we call $\mathrm{ann}(f) = \{L \in A : L \cdot f = 0\}$ the *annihilator* of f (in A).
2. $f \in F$ is called *D-finite* (with respect to the action of A on F) if the K-vector space $A \cdot f = \{L \cdot f : L \in A\} \subseteq F$ has finite dimension. □

Example 4.64

1. If $\mathbb{Q}(x,y)[D_x, D_y]$ acts on the function space F of all bivariate meromorphic functions, then the element $\exp(x+y) \in F$ is D-finite. Its annihilator contains the operators $D_x - 1$ and $D_y - 1$, so the vector space $\mathbb{Q}(x,y)[D_x, D_y]\cdot\exp(x+y)$ consists of all $\mathbb{Q}(x,y)$-multiples of $\exp(x+y)$ and thus has dimension 1.

The element $f = x + \exp(x + y) \in F$ is also D-finite. Its annihilator contains the operators $(1 - x)D_x^2 + xD_x - 1$ and $D_y^2 - D_y$, which can be used to rewrite each derivative $D_x^i D_y^j \cdot f$ as a $\mathbb{Q}(x, y)$-linear combination of f, $D_x \cdot f$, $D_y \cdot f$, $D_x D_y \cdot f$. We therefore have $\dim_{\mathbb{Q}(x,y)} \mathbb{Q}(x, y)[D_x, D_y] \cdot f \le 4$. The actual dimension is smaller because there are additional relations. Another element of the annihilator is $xD_x + (1 - x)D_y - 1$, and this element can be used to rewrite $D_x \cdot f$ and $D_x D_y \cdot f$ as linear combinations of f and $D_y \cdot f$, so these two functions also generate the $\mathbb{Q}(x, y)$-vector space $\mathbb{Q}(x, y)[D_x, D_y] \cdot f$. In fact, they form a basis and the dimension of the space is 2.

2. Let F be the set of germs of bivariate sequences, i.e., the set of all equivalence classes of sequences $a\colon \mathbb{N} \times \mathbb{N} \to C$ modulo the equivalence relation that identifies all sequences that differ on the vanishing set of a nonzero bivariate polynomial (cf. Definition 1.13). If we let the Ore algebra $C(n, k)[S_n, S_k]$ act on F, then the binomial coefficient $\binom{n}{k}$, viewed as an element of F, is D-finite. Its annihilator contains the operators $(1+n)-(1-k+n)S_n$ and $(k-n)+(k+1)S_k$, reflecting the identities

$$\binom{n+1}{k} = \frac{n+1}{n-k+1}\binom{n}{k} \quad \text{and} \quad \binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}.$$

These identities show that for each $i, j \in \mathbb{N}$, we can rewrite $S_n^i S_k^j \cdot \binom{n}{k}$ as a $C(n, k)$-multiple of $\binom{n}{k}$. Hence $\dim_{C(n,k)} C(n, k)[S_n, S_k] \cdot \binom{n}{k} = 1$.

The element $f = 1 + \binom{n}{k} \in F$ is also D-finite. Its annihilator contains the operators

$$(n - k + 2)S_n^2 - (2n - k + 3)S_n + (n + 1) \quad \text{and}$$
$$(k + 2)(1 + 2k - n)S_k^2 - (2k + 2 - n)(n + 1)S_k - (k - n)(3 + 2k - n).$$

With these operators, every term $S_n^i S_k^j \cdot f$ can be rewritten as a linear combination of f, $S_n \cdot f$, $S_k \cdot f$, $S_n S_k \cdot f$, so $\dim_{C(n,k)} C(n, k)[S_n, S_k] \cdot f \le 4$. Like in the previous example, the dimension is actually smaller. Because of the additional annihilating operator

$$(n - k + 1)(1 + 2k - n)S_n + k(k + 1)S_k + (n^2 - 3kn + k^2 - 2k - 1),$$

the vector space $C(n, k)[S_n, S_k] \cdot f$ is already generated by f and $S_k \cdot f$. In fact they form a basis.

The Stirling numbers of the second kind $S_2(n, k)$ are annihilated by the operator $S_n S_k - (k+1)S_k - 1 \in C(n, k)[S_n, S_k]$. With this operator, every element $S_n^i S_k^j \cdot S_2(n, k)$ can be rewritten as a $C(n, k)$-linear combination of terms $S_n^p \cdot S_2(n, k)$ and $S_k^q \cdot S_2(n, k)$ for various $p, q \in \mathbb{N}$, but these terms can be shown to be linearly independent, and since there are infinitely many, the Stirling numbers are not D-finite even though their annihilator is not empty.

3. Let F be the set of all germs of univariate sequences in $C(x)$, and let $C(x,n)[D_x, S_n]$ act on F. The sequence $(P_n(x))_{n=0}^{\infty}$ of Legendre polynomials, viewed as an element of F, is D-finite. This sequence is defined recursively by $P_0(x) = 1$, $P_1(x) = x$, and

$$(n+2)P_{n+2}(x) - (2n+3)xP_{n+1}(x) + P_n(x) = 0 \qquad (n \in \mathbb{N}).$$

This recurrence alone implies that the sequence $(P_n(x))_{n=0}^{\infty}$ is D-finite with respect to the action of $C(x,n)[S_n]$, in other words, it is D-finite in the sense of Chap. 2. With respect to the action of $C(x,n)[D_x, S_n]$, the recurrence only allows us to rewrite any term $D_x^i S_n^j \cdot P_n(x)$ as a linear combination of terms $D_x^k \cdot P_n(x)$ and $D_x^\ell S_n \cdot P_n(x)$ for various $k, \ell \in \mathbb{N}$. There are infinitely many of these terms, but there is an additional annihilating operator $(1-x^2)D_x + (n+1)S_n - (n+1)x$ of $P_n(x)$, so $P_n(x)$ and $S_n \cdot P_n(x)$ already generate the whole $C(x,n)$-vector space $C(x,n)[D_x, S_n] \cdot P_n(x)$. □

In these examples, we can see that the dimension of $K[\partial_1, \ldots, \partial_n] \cdot f$ is finite by finding, for each i, an annihilating operator containing ∂_i but none of the other generators. The following proposition says that this works in general. Informally speaking, a multivariate object is D-finite if and only if it is D-finite as a univariate object for each of the variables.

Proposition 4.65 *Let $A = K[\partial_1, \ldots, \partial_n]$ be an Ore algebra over a field K and let F be an A-module. An element $f \in F$ is D-finite if and only if* $\operatorname{ann}(f) \cap K[\partial_i] \neq \{0\}$ *for all $i = 1, \ldots, n$.* □

Proof "⇒": If f is D-finite, then $\dim_K(A \cdot f) =: d < \infty$, so for every $i = 1, \ldots, n$, the elements $f, \partial_i \cdot f, \cdots, \partial_i^d \cdot f \in F$ are linearly dependent over K. The linear dependence corresponds to a nonzero element of $\operatorname{ann}(f) \cap K[\partial_i]$.

"⇐": If $\operatorname{ann}(f) \cap K[\partial_i] \neq \{0\}$ for all $i = 1, \ldots, n$, we can let $r_i \in \mathbb{N}$ $(i = 1, \ldots, n)$ be such that $\operatorname{ann}(f) \cap K[\partial_i]$ contains an operator of order r_i. Using these operators, every term $\partial_1^{p_1} \cdots \partial_n^{p_n} \cdot f$ $(p_1, \ldots, p_n \in \mathbb{N})$ can be rewritten into a K-linear combination of terms $\partial_1^{q_1} \cdots \partial_n^{q_n} \cdot f$ with $0 \le q_i < r_i$ $(i = 1, \ldots, n)$. Since there are only finitely many of such terms, it follows that $\dim_K(A \cdot f) < \infty$, so f is D-finite. ■

In the univariate case, a D-finite series or sequence is uniquely determined by an annihilating operator and a finite number of initial terms. One of the motivations behind Definition 4.63 is to have the same feature also in the case of several variables. Indeed, as long as no trouble is caused by singularities, the generalization is very natural. For notational simplicity, let us consider the case of two variables. In the differential case, consider a left ideal $I \subseteq C(x,y)[D_x, D_y]$ such that $\dim_{C(x,y)} C(x,y)[D_x, D_y]/I$ is finite, and let $B_1, \ldots, B_r \in C(x,y)[D_x, D_y]$ be such that their equivalence classes form a vector space basis of $C(x,y)[D_x, D_y]/I$. A bivariate formal power series $a(x,y) = \sum_{n,k=0}^{\infty} a_{n,k} x^n y^k \in C[x,y]$ is called a *solution* of I if $I \subseteq \operatorname{ann} a(x,y)$. For every $i, j \in \mathbb{N}$, there are $u_1, \ldots, u_r \in C(x,y)$

such that $D_x^i D_y^j$ is equivalent modulo I to $u_1 B_1 + \cdots + u_r B_r$. For any coefficient $a_{i,j}$ of a solution $a(x, y)$ of I, we must therefore have

$$\begin{aligned} a_{i,j} &= [x^i y^j]a(x, y) = \frac{1}{i!j!}\big(D_x^i D_y^j \cdot a(x, y)\big)\big|_{x=y=0} \\ &= \frac{1}{i!j!}\big((u_1 B_1 + \cdots + u_r B_r) \cdot a(x, y)\big)\big|_{x=y=0}. \end{aligned}$$

As long as the denominators of the u_ℓ or the B_ℓ do not vanish for $x = y = 0$, all of these coefficients are uniquely determined once we know the finitely many values $(B_\ell \cdot a(x, y))|_{x=0,y=0}$ ($\ell = 1, \ldots, r$). Conversely, every choice of constants $(B_\ell \cdot a(x, y))|_{x=0,y=0}$ ($\ell = 1, \ldots, r$) gives rise to a solution of I.

If some of the B_ℓ have denominators that vanish for $x = y = 0$ or there are some $i, j \in \mathbb{N}$ for which the corresponding u_ℓ have denominators that vanish for $x = y = 0$, then we say that $(0, 0)$ is a singular point of I. In this case, it can be difficult to determine which initial values give rise to power series solutions. Note that whether $(0, 0)$ is a singularity or not depends not only on the ideal I, but also on the choice of the basis $B_1, \ldots, B_\ell$.

In the shift case, the situation is similar. Given a left ideal $I \subseteq C(n, k)[S_n, S_k]$ for which the dimension of $C(n, k)[S_n, S_k]/I$ is finite, and operators $B_1, \ldots, B_r \in C(n, k)[S_n, S_k]$ whose equivalence classes form a basis of $C(n, k)[S_n, S_k]/I$, a bivariate sequence $(a_{n,k})_{n,k=0}^\infty$ is a solution of I if $I \subseteq \operatorname{ann}(a_{n,k})_{n,k=0}^\infty$. For every $i, j \in \mathbb{N}$, there are $u_1, \ldots, u_r \in C(n, k)$ such that $S_n^i S_k^j$ is equivalent modulo I to $u_1 B_1 + \cdots + u_r B_r$, so for any solution $(a_{n,k})_{n,k=0}^\infty$ we must have

$$\begin{aligned} a_{i,j} &= (a_{n,k})_{n,k=0}^\infty\big|_{n=i,k=j} = (a_{n+i,k+j})_{n,k=0}^\infty\big|_{n=k=0} \\ &= \big(S_n^i S_k^j \cdot (a_{n,k})_{n,k=0}^\infty\big)\big|_{n=k=0} = \big((u_1 B_1 + \cdots + u_r B_r) \cdot (a_{n,k})_{n,k=0}^\infty\big)\big|_{n=k=0}. \end{aligned}$$

Like before, trouble arises only if the u_ℓ or the B_ℓ cannot be evaluated at $n = k = 0$ because of vanishing denominators. Such trouble is not uncommon.

Example 4.66

1. Consider the ideal

$$I = \langle nS_n - (n + k), S_k - (n + k)\rangle \subseteq C(n, k)[S_n, S_k].$$

The vector space $C(n, k)[S_n, S_k]/I$ is generated by the equivalence class of $B = 1 = S_n^0 S_k^0$. If there is no singularity trouble, every choice $a_{0,0} \in C$ can be uniquely extended to a solution $(a_{n,k})_{n,k=0}^\infty$ of I. However, there is singularity trouble: for every $i, j \in \mathbb{N}$, we have

$$S_n^i S_k^j - \frac{(n+k)(n+k+1)\cdots(n+k+i+j-1)}{n(n+1)\cdots(n+i-1)} \in I,$$

and an attempt to evaluate

$$a_{i,j} = \Big(\frac{(n+k)(n+k+1)\cdots(n+k+i+j-1)}{n(n+1)\cdots(n+i-1)} a_{n,k}\Big)\Big|_{n=k=0}$$

for some $i, j \in \mathbb{N}$ with $i > 0$ leads to a division by zero. We can only conclude that $a_{0,j} = 0$ for all $j > 0$. More generally, if we know all terms $a_{i,0}$ ($i \in \mathbb{N}$) of a solution, the formula above lets us compute all other terms. But there are infinitely many initial values.

The equivalence class of the operator S_n is also a basis of the vector space $C(n,k)[S_n, S_k]/I$. For every $i, j \in \mathbb{N}$ with $i > 0$ we have $S_n^i S_k^j - r_{i,j} S_n \in I$, where

$$r_{i,j} = \begin{cases} \frac{(n+k+1)(n+k+2)\cdots(n+k+i+j-1)}{(n+1)(n+2)\cdots(n+i-1)} & \text{if } i > 0, \\ n(n+k+1)(n+k+2)\cdots(n+k+i+j-1) & \text{if } i = 0 \text{ and } j > 0, \\ \frac{n}{k+n} & \text{if } i = j = 0. \end{cases}$$

The attempt to evaluate $a_{i,j} = (r_{i,j} a_{n+1,k})|_{n=k=0}$ will succeed for every $i, j \in \mathbb{N}$ except for $(i, j) = (0, 0)$. Therefore, a sequence solution of I is uniquely determined by the single initial value $a_{1,0}$ and the isolated exceptional term $a_{0,0}$.

2. Consider the ideal $I = \langle (k-n)S_n + (n-k+1), (k-n)S_k + (n-k-1)\rangle \subseteq C(n,k)[S_n, S_k]$. Again the vector space $C(n,k)[S_n, S_k]/I$ has dimension 1 and every nonzero element of it can serve as a basis. Again, some bases are better than others.

   Taking $B = 1$, we find that $S_n^i S_k^j - \frac{k+j-n-i}{k-n} \in I$, but evaluating $a_{i,j} = (\frac{k+j-n-i}{k-n} a_{n,k})|_{n=k=0}$ fails for every choice $i, j \in \mathbb{N}$ with $i \neq j$. Taking any other monomial $S_n^u S_k^v$ with $u \neq v$ as B solves the problem, because $S_n^i S_k^j - \frac{k+j-n-i}{k+v-n-u} S_n^u S_k^v \in I$ leads to evaluating $a_{i,j} = (\frac{k+j-n-i}{k+v-n-u} a_{n+u,k+v})_{n=k=0}$, which succeeds when $u \neq v$. □

The examples above were chosen so that it was possible to resolve the problems caused by singularities. This is not always possible, and it is not always easy to decide whether it is possible or not, especially if the vector space dimension is greater than one. Such issues are part of the price we have to pay for working with an Ore algebra $K[\partial_1, \ldots, \partial_n]$ defined over a field K. If we are in a situation where we are not willing to pay this price, we are led to the notion of holonomy (also known as holonomicity), a concept closely related but not equivalent to D-finiteness. Its definition is motivated by Proposition 4.65.

Definition 4.67 Let $A = C[x_1, \ldots, x_n][\partial_1, \ldots, \partial_n]$ be an Ore algebra, let I be a left ideal of A, and let f be an element of an A-module F.

1. I is called *holonomic* if for every subset $U \subseteq \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$ with $|U| = n + 1$ we have $I \cap C[U] \neq \{0\}$.
2. f is called *holonomic* if the ideal $\operatorname{ann}(f) = \{L \in A : L \cdot f = 0\} \subseteq A$ is holonomic. □

One feature of holonomy is that it can also describe "functions" that are zero almost everywhere. For example, an object $\delta(x, y)$ which is zero except when $x = y$ is annihilated by the operator $x - y \in C[x, y][D_x, D_y]$. A meromorphic function cannot be of this form, but suitably generalized notions of functions such as distributions may be. Note that we cannot formulate the annihilation of a nonzero object by $x - y$ in the Ore algebra $C(x, y)[D_x, D_y]$ because $x - y \in \operatorname{ann}(f)$ implies $\frac{1}{x-y}(x - y) = 1 \in \operatorname{ann}(f)$, which means $1 \cdot f = f = 0$.

Example 4.68

1. $x + \exp(xy^2) \in C[[x, y]]$ is holonomic with respect to the algebra $C[x, y][D_x, D_y]$ because its annihilator contains the operators

$$\begin{aligned}
L_1 &= xy^2 D_x^2 - D_x^2 - xy^4 D_x + y^4 && \in C[x, y][D_x] \subseteq C[x, y][D_x, D_y],\\
L_2 &= y D_y^2 - D_y - 2xy^2 D_y && \in C[x, y][D_y] \subseteq C[x, y][D_x, D_y],\\
L_3 &= D_y^3 - 4x^2 D_x D_y - 2x D_y && \in C[x][D_x, D_y] \subseteq C[x, y][D_x, D_y],\\
L_4 &= D_x^3 - y^2 D_x^2 && \in C[y][D_x, D_y] \subseteq C[x, y][D_x, D_y].
\end{aligned}$$

2. $\binom{n}{k}$ is holonomic with respect to $C[n, k][S_n, S_k]$ because its annihilator contains the operators

$$\begin{aligned}
L_1 &= (n - k + 1)S_n - (n + 1) && \in C[n, k][S_n],\\
L_2 &= (k + 1)S_k - (k - n) && \in C[n, k][S_k],\\
L_3 &= S_n S_k - S_k - 1 && \in C[n][S_n, S_k],\\
L_4 &= S_n S_k - S_k - 1 && \in C[k][S_n, S_k].
\end{aligned}$$

□

According to Proposition 4.65, an object is already D-finite if it has annihilating operators like the operators L_1 and L_2 in the examples above, and since holonomic objects must in addition have annihilating operators like L_3 and L_4, it seems that holonomy is a stronger requirement than D-finiteness. However, this is not necessarily the case. We will show next that if the Ore algebra is such that all σ_i are equal to id (like for example in the differential case), holonomy is in fact equivalent to D-finiteness. In the proof, we will construct the required operators by setting up a linear system with more variables than equations, as we have already done many times. This time however, we will use a linear system over C rather than over K.

Theorem 4.69 *Let $A = C[x_1, \ldots, x_n][\partial_1, \ldots, \partial_n]$ be an Ore algebra with $\sigma_1 = \cdots = \sigma_n = \mathrm{id}$. Let F be a $C[x_1, \ldots, x_n][\partial_1, \ldots, \partial_n]$-module which can also be viewed as a $C(x_1, \ldots, x_n)[\partial_1, \ldots, \partial_n]$-module, and let $f \in F$. Then f is holonomic if and only if it is D-finite.* □

Proof "⇒": If f is holonomic, then for every $i = 1, \ldots, n$ there exists a nonzero annihilating operator in $C[x_1, \ldots, x_n][\partial_i] \subseteq C(x_1, \ldots, x_n)[\partial_i]$. From Proposition 4.65 it follows that f is D-finite.

"⇐": Write $K = C(x_1, \ldots, x_n)$ and let $B = \{b_1, \ldots, b_r\}$ be a basis of the K-vector space $V = K[\partial_1, \ldots, \partial_n] \cdot f \subseteq F$. Without loss of generality, we may assume $b_1 = f$. To every element $g = u_1 b_1 + \cdots + u_r b_r$ of V we associate the coefficient vector $\hat{g} = (u_1, \ldots, u_r) \in K^r$ with respect to B. There are matrices $A_1, \ldots, A_n \in K^{r \times r}$ such that the coefficient vector of $\partial_i \cdot g$ is $A_i \hat{g} + \delta_i(\hat{g})$ ($i = 1, \ldots, n$), where $\delta_i(\hat{g})$ means componentwise application of δ_i.

Let q be a common denominator of all entries of all A_i ($i = 1, \ldots, n$), and let $d \geq 1$ be such that the total degree of q as well as the entries of the qA_i ($i = 1, \ldots, n$) are less than d. For an element $g \in V$ with $\hat{g} = q^{-k}(p_1, \ldots, p_r)$ for some $k \in \mathbb{N}$, and certain polynomials $p_1, \ldots, p_r \in C[x_1, \ldots, x_n]$ of total degree at most $u \in \mathbb{N}$, the coefficient vector of any $\partial_i \cdot g$ will have the form $q^{-(k+1)}(\tilde{p}_1, \ldots, \tilde{p}_r)$ for certain polynomials $\tilde{p}_1, \ldots, \tilde{p}_r \in C[x_1, \ldots, x_n]$ of total degree at most $u + d$. (Here we used that $\sigma_i = \mathrm{id}$.) Also the coefficient vector of any $x_i \cdot g$ has this format. By induction, it follows that for every $k \in \mathbb{N}$ and every choice $i_1, \ldots, i_n, j_1, \ldots, j_n \in \mathbb{N}$ with $i_1 + \cdots + i_n + j_1 + \cdots + j_n \leq k$, the coefficient vector of

$$x_1^{i_1} \cdots x_n^{i_n} \partial_1^{j_1} \cdots \partial_n^{j_n} \cdot f \in V$$

has the form $q^{-k}(p_1, \ldots, p_r)$ for certain polynomials $p_1, \ldots, p_r \in C[x_1, \ldots, x_n]$ of total degree at most kd.

Now let $U \subseteq \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$ with $|U| = n + 1$. We have to show that f has an annihilating operator in $C[U]$. For a $k \in \mathbb{N}$, consider an ansatz $L = \sum_\tau c_\tau \tau$ for such an operator, where τ ranges over all terms $x_1^{i_1} \cdots x_n^{i_n} \partial_1^{j_1} \cdots \partial_n^{j_n}$ with $i_1 + \cdots + i_n + j_1 + \cdots + j_n \leq k$ but only involving variables from U (i.e., $i_\ell = 0$ if $x_\ell \notin U$ and $j_\ell = 0$ if $\partial_\ell \notin U$). Because of $|U| = n + 1$, the ansatz for L contains $\binom{n+1+k}{k}$ undetermined coefficients c_τ. By the analysis in the previous paragraph, the coefficient vector of $L \cdot f$ with respect to the basis B has the form $q^{-k}(p_1, \ldots, p_r)$ for certain $p_1, \ldots, p_r \in C[x_1, \ldots, x_n]$ of total degree at most kd. Equating the coefficients of all the p_i ($i = 1, \ldots, r$) with respect to the variables $x_1, \ldots, x_n$ to zero yields a linear system over C with at most $r\binom{n+kd}{kd}$ equations.

For sufficiently large k, we have $\binom{n+1+k}{k} > r\binom{n+kd}{kd}$, because the left hand side is a polynomial in k of degree $n + 1$ (with a positive leading coefficient) while the right hand side is a polynomial in k of degree n. Therefore, when k is sufficiently large, the linear system will have a nonzero solution. This solution gives rise to the required nonzero operator L. ■

The restriction on the σ_i in the theorem above ensures that the rational functions appearing in the proof have a small common denominator. If the common denominator is small, the corresponding numerators are also small, and this means that coefficient comparison does not lead to too many equations. If some σ_i are different from id, as for example in the shift case, holonomy and D-finiteness are not the same.

Example 4.70 The rational function $a(n,k) = 1/(n^2+k^2)$ is D-finite because it satisfies the recurrence equations

$$(n^2+(k+1)^2)a(n,k+1) - (n^2+k^2)a(n,k) = 0,$$
$$((n+1)^2+k^2)a(n+1,k) - (n^2+k^2)a(n,k) = 0.$$

It is however not holonomic, because in order for $a(n,k)$ to be holonomic, we would also need an annihilating operator only containing n, S_k, S_n, i.e., a relation of the form

$$\sum_{u,v} \frac{p_{u,v}(n)}{(n+u)^2+(k+v)^2} = 0$$

for certain polynomials $p_{u,v}$, not all zero. Such a relation does not exist. To see why, suppose there is a pair (i,j) for which $p_{i,j}$ is not the zero polynomial. Then there is an $m \in \mathbb{Q}\setminus\mathbb{Z}$ such that $p_{i,j}(m) \neq 0$, so setting n to m in the relation above yields a C-linear dependence among the rational functions $1/((m+u)^2+(k+v)^2) \in C(k)$. But these rational functions are C-linearly independent because their denominators are pairwise coprime. See Exercise 8 for some more details. □

The lack of equivalence between holonomy and D-finiteness in the shift case can be a source of annoyance. For example, it can be shown (Exercise 5) that a sequence $(a_{n,k})_{n,k=0}^{\infty}$ is holonomic with respect to $C[n,k][S_n,S_k]$ if and only if its generating function $a(x,y) = \sum_{n,k=0}^{\infty} a_{n,k}x^n y^k$ is holonomic with respect to $C[x,y][D_x,D_y]$. The latter is equivalent to D-finiteness but, as we have just seen, the former is not. This means that Theorem 2.33 for translating recurrence equations to differential equations does not carry over to multivariate D-finite functions. Summation and integration also do not preserve D-finiteness in the case of several variables. For example, $\frac{1}{n+x}$ is D-finite with respect to $C(n,x)[S_n,D_x]$ but $\int \frac{1}{n+x}dx$ and $\sum_{k=1}^{n} \frac{1}{k+x}$ are not (Exercises 2 and 12).

Summation and integration are the subject of the next chapter. Other closure properties are less problematic. In particular, addition and (if meaningful) multiplication preserve D-finiteness.

Theorem 4.71 *Let $A = K[\partial_1,\dots,\partial_n]$ be an Ore algebra and F be an A-module. Let $f, g \in F$ be D-finite.*

1. *$L \cdot f$ is D-finite for every $L \in A$.*
2. *$f + g$ is D-finite.*

3. *If $m\colon F \times F \to F$ is a K-bilinear function such that for every $i = 1, \dots, n$ there are $\alpha_i, \beta_i, \gamma_i \in K$ with*

$$\partial_i \cdot m(u, v) = \alpha_i m(u, v) + \beta_i m(\partial_i \cdot u, v) + \beta_i m(u, \partial_i \cdot v) + \gamma_i m(\partial_i \cdot u, \partial_i \cdot v)$$

for all $u, v \in F$. Then $m(f, g)$ is D-finite. □

Proof

1. Since f is D-finite, $\dim_K(A \cdot f) < \infty$. $A \cdot (L \cdot f)$ is a subspace of $A \cdot f$ and therefore also has finite dimension. The claim follows.
2. Since f, g are D-finite, we have $\dim_K(A \cdot f), \dim_K(A \cdot g) < \infty$. Consequently, $\dim_K(A \cdot f + A \cdot g) < \infty$. The K-vector space $A \cdot (f + g)$ is a subspace of $A \cdot f + A \cdot g$ and therefore also has a finite dimension. The claim follows.
3. Since f, g are D-finite, we have $\dim_K(A \cdot f), \dim_K(A \cdot g) < \infty$. Consequently, $\dim_K((A \cdot f) \otimes_K (A \cdot g)) < \infty$. By the assumption on m, the K-vector space $A \cdot m(f, g)$ is isomorphic to (a subspace of) $(A \cdot f) \otimes_K (A \cdot g)$ and therefore also has a finite dimension. The claim follows. ■

Theorem 4.72

1. *Let $f \in C[[x_1, \dots, x_n]]$ be D-finite (with respect to the algebra $C(x_1, \dots, x_n)[D_{x_1}, \dots, D_{x_n}]$) and suppose that elements $g_1, \dots, g_n \in C[[z_1, \dots, z_m]]$ are algebraic over $C(z_1, \dots, z_m)$ but algebraically independent over C. If the composition $f(g_1, \dots, g_n)$ is a well-defined element of $C[[z_1, \dots, z_m]]$, then it is D-finite (w.r.t. $C(z_1, \dots, z_m)[D_{z_1}, \dots, D_{z_m}]$).*
2. *Let $f\colon \mathbb{C}^n \to \mathbb{C}$ be a meromorphic D-finite function (with respect to the algebra $C(x_1, \dots, x_n)[S_{x_1}, \dots, S_{x_n}]$). Suppose that linear functions $g_1, \dots, g_n\colon \mathbb{Q}^m \to \mathbb{Q}$ are linearly independent over $\mathbb{C}$. Then the composition $f(g_1, \dots, g_n)$ is D-finite (w.r.t. $C(z_1, \dots, z_m)[S_{z_1}, \dots, S_{z_m}]$).* □

Proof

1. The field $C(z_1, \dots, z_m)(g_1, \dots, g_n)$ is closed under application of D_{z_i} for every $i = 1, \dots, m$ (for the same reason as in the univariate case), and it is a finite-dimensional $C(z_1, \dots, z_m)$-vector space (also for the same reason as in the univariate case).
   Since f is D-finite, the functions $D_{x_1}^{e_1} \cdots D_{x_n}^{e_n} \cdot f$ form a finite-dimensional $C(x_1, \dots, x_n)$-vector space. The substitution $x_i \mapsto g_i$ ($i = 1, \dots, n$) is well-defined on this space, because $g_1, \dots, g_n$ are assumed to be algebraically independent over C, so plugging them into the denominator of an element of $C(x_1, \dots, x_n)$ cannot produce a division by zero. Therefore, the functions $(D_{x_1}^{e_1} \cdots D_{x_n}^{e_n} \cdot f)(g_1, \dots, g_n)$ form a finite-dimensional $C(g_1, \dots, g_n)$-vector space, which we may also view as a $C(z_1, \dots, z_m)(g_1, \dots, g_n)$-vector space. Call this space V.
   For $h = f(g_1, \dots, g_n)$, we have

$$D_{z_i} \cdot h = \sum_{j=1}^{n} \underbrace{\underbrace{\big((D_{x_j} \cdot f)(g_1, \ldots, g_n)\big)}_{\in V} \quad \overbrace{(D_{z_i} \cdot g_j)}^{\in C(z_1,\ldots,z_m)(g_1,\ldots,g_n)}}_{\in V} \qquad \in V$$

for every $i = 1, \ldots, m$, by the chain rule. By induction, it follows that every $D_{z_1}^{e_1} \cdots D_{z_m}^{e_m} \cdot h$ belongs to V. Since V is a finite-dimensional vector space over $C(z_1, \ldots, z_m)(g_1, \ldots, g_n)$ and $C(z_1, \ldots, z_m)(g_1, \ldots, g_n)$ is a finite-dimensional vector space over $C(z_1, \ldots, z_m)$, V is a finite-dimensional $C(z_1, \ldots, z_m)$-vector space, and since V contains $C(z_1, \ldots, z_m)[D_{z_1}, \ldots, D_{z_m}] \cdot h$ as a subspace, we have shown that h is D-finite.

2. Using vector notation $z = (z_1, \ldots, z_m)$, $g = (g_1, \ldots, g_n)$, etc., we can write

$$S_{z_i} \cdot f(g(z)) = f(g(z) + g(e_i)) \qquad (i = 1, \ldots, m),$$

where e_i is the ith unit vector in $\mathbb{C}^n$. More generally, for every choice $\ell_1, \ldots, \ell_m \in \mathbb{N}$ we have

$$S_{z_1}^{\ell_1} \cdots S_{z_m}^{\ell_m} \cdot f(g(z)) = f(g(z) + \ell_1 g(e_1) + \cdots + \ell_m g(e_m)).$$

If $d \in \mathbb{N}$ is the common denominator of the entries of $g(e_1), \ldots, g(e_m) \in \mathbb{Q}^n$, we find that each $S_{z_1}^{\ell_1} \cdots S_{z_m}^{\ell_m} \cdot f(g(z))$ belongs to the $C(x_1, \ldots, x_n)$-vector space generated by $f(g(z) + u/d)$, where u runs through $\mathbb{N}^n$. Since f is D-finite, this space is also generated by $f(g(z) + u/d)$ where u runs through $\{0, \ldots, r\}^n$ for some sufficiently large $r \in \mathbb{N}$. Hence, its dimension is finite.

The substitution $x_i \mapsto g_i$ $(i = 1, \ldots, n)$ is well-defined on this space, because the assumption on $g_1, \ldots, g_n$ implies that these functions are algebraically independent over C (Exercise 14), so plugging them into the denominator of an element of $C(x_1, \ldots, x_n)$ cannot produce a division by zero. Therefore, the $C(z_1, \ldots, z_m)$-vector space $C(z_1, \ldots, z_m)[S_{z_1}, \ldots, S_{z_m}] \cdot f(g)$ has finite dimension, which proves that $f(g)$ is D-finite. ∎

The condition of algebraic independence on the substitution arguments is required only for ensuring that there is no division by zero. If there is a dependence between the arguments, there is a good chance that the computation succeeds nevertheless, and it is worth giving it a try. If it fails, more advanced techniques discussed in the next chapter can be applied (cf. Theorems 5.30 and 5.36). In particular, these more advanced techniques are often needed when one of the arguments is set to a constant, e.g., when we want to compute a differential equation in x for $f(x, 0)$ from a system of differential equations in x, y for $f(x, y)$.

For the shift case, we have formulated the closure under substitution for meromorphic functions rather than sequences because this case can be formulated more conveniently. For sequences, we would have to restrict to substitutions that map (nonnegative) integer arguments to (nonnegative) integer arguments, but the proof is otherwise the same. We have furthermore simplified matters by considering only the pure differential case and the pure shift case, respectively. The result can be extended to the mixed case, as long as it is ensured that the substitution only affects variables on which only derivations or shifts act. For example, given a D-finite element $f(x_1, x_2, n_1, n_2, u_1, u_2)$ of a module on which an Ore algebra $C(x_1, x_2, n_1, n_2, u_1, u_2)[D_{x_1}, D_{x_2}, S_{n_1}, S_{n_2}, \partial_{u_1}, \partial_{u_2}]$ acts, a substitution $x_1 = g_1(z_1, z_2)$, $x_2 = g_2(z_1, z_2)$, $n_1 = h_1(k_1, k_2)$, $n_2 = h_2(k_1, k_2)$ with g_1, g_2 algebraic and algebraically independent and h_1, h_2 linear and linearly independent yields a result which is D-finite with respect to the Ore algebra $C(z_1, z_2, k_1, k_2, u_1, u_2)[D_{z_1}, D_{z_2}, S_{k_1}, S_{k_2}, \partial_{u_1}, \partial_{u_2}]$.

Closure properties are easy to program if we do not represent a D-finite function f using annihilating operators but instead exploit that the K-vector space $K[\partial_1, \ldots, \partial_n] \cdot f$ has finite dimension. To have a finite dimension means that for some $r \in \mathbb{N}$ there is a K-vector space embedding $\phi\colon K[\partial_1, \ldots, \partial_n] \cdot f \to K^r$. Like in the proof of Theorem 4.69, we can turn K^r into a $K[\partial_1, \ldots, \partial_n]$-module and ϕ into a module homomorphism by choosing matrices $A_1, \ldots, A_n \in K^{r\times r}$ such that

$$\phi(\partial_i \cdot u) = A_i \sigma_i(\phi(u)) + \delta_i(\phi(u))$$

for $i = 1, \ldots, n$ and every $u \in K[\partial_1, \ldots, \partial_n] \cdot f$, where the applications of the σ_i and δ_i are meant componentwise. We call these matrices *companion matrices* for $\partial_1, \ldots, \partial_n$. Depending on the circumstances, it may be fair to say that we know the D-finite function f once we know the vector $\phi(f) \in K^r$, the companion matrices, and the functions $\sigma_1, \ldots, \sigma_n, \delta_1, \ldots, \delta_n$ defining the Ore algebra.

With this point of view, if f, g are two D-finite functions and we have module embeddings $\phi\colon K[\partial_1, \ldots, \partial_n] \cdot f \to K^r$ and $\psi\colon K[\partial_1, \ldots, \partial_n] \cdot g \to K^s$ with companion matrices $A_1, \ldots, A_n \in K^{r\times r}$ and $B_1, \ldots, B_n \in K^{s\times s}$, then we can encode $h := f + g$ by the embedding $\chi\colon K[\partial_1, \ldots, \partial_n] \cdot h \to K^{r+s}$ defined by $\chi(h) = \binom{\phi(f)}{\psi(g)} \in K^{r+s}$ and the companion matrices

$$\begin{pmatrix} A_1 & \\ & B_1 \end{pmatrix}, \ldots, \begin{pmatrix} A_n & \\ & B_n \end{pmatrix} \in K^{(r+s)\times(r+s)}.$$

This takes literally no computation time. For other closure properties, the construction is only slightly more involved.

If a D-finite function f is given in the sense outlined above, i.e., if for a certain module embedding $\phi\colon K[\partial_1, \ldots, \partial_n] \cdot f \to K^r$ we know the vector $\phi(f) \in K^r$ and the companion matrices $A_1, \ldots, A_n \in K^{r\times r}$ describing the action of $\partial_1, \ldots, \partial_n$ on K^r, we can also compute generators of the ideal $\operatorname{ann}(f) \subseteq K[\partial_1, \ldots, \partial_n]$. This works as follows. First observe that for any given term $\partial_1^{e_1} \cdots \partial_n^{e_n}$ we can use $\phi(f)$ as well as the companion matrices $A_1, \ldots, A_n$ to compute the vector $\phi(\partial_1^{e_1} \cdots \partial_n^{e_n} \cdot f) \in K^r$. Therefore, given any finite number of such terms, say $\tau_1, \ldots, \tau_m$, we can decide whether f has an annihilating operator consisting of these terms by checking whether the vectors $\phi(\tau_1 \cdot f), \ldots, \phi(\tau_m \cdot f) \in K^r$ are linearly dependent over K.

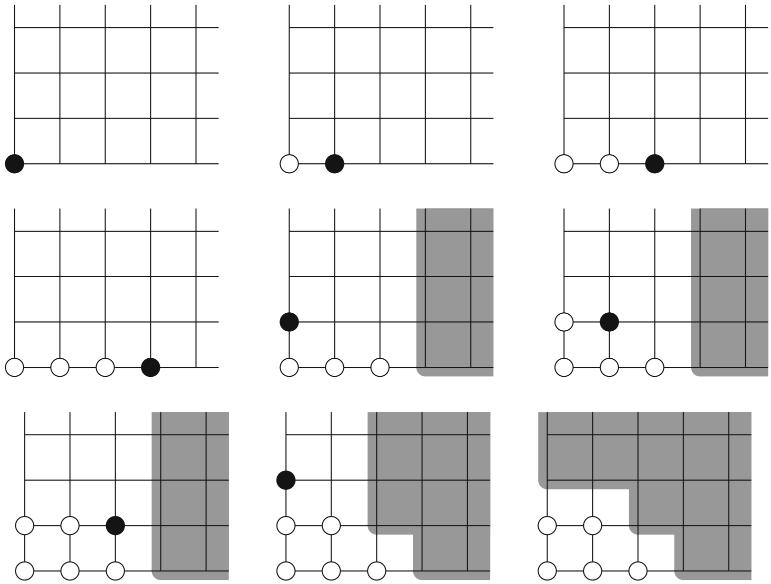
Clearly, for any $p_1, \ldots, p_m \in K$ we have $p_1\tau_1 + \cdots + p_m\tau_m \in \operatorname{ann}(f)$ if and only if $(p_1\tau_1 + \cdots + p_m\tau_m) \cdot f = 0$ if and only if $\phi((p_1\tau_1 + \cdots + p_m\tau_m) \cdot f) = 0$ (since ϕ is supposed to be injective) if and only if $p_1\phi(\tau_1 \cdot f) + \cdots + p_m\phi(\tau_m \cdot f) = 0$.

Secondly, we need a systematic way to choose candidate terms $\tau_1, \ldots, \tau_m$. On the set of all terms $\partial_1^{e_1} \cdots \partial_n^{e_n}$, we define an ordering $\leq$ with the property that $1 = \partial_1^0 \cdots \partial_n^0$ is the smallest element and $\tau_1 \leq \tau_2 \Rightarrow \sigma\tau_1 \leq \sigma\tau_2$ for all terms σ, τ_1, τ_2. Such an order is called a *term order.* With respect to a term order, every nonzero operator $L \in K[\partial_1, \ldots, \partial_n]$ has a maximal term, called the *leading term* of the operator and denoted by $\operatorname{lt}(L)$. By the second defining property of term orders, we have $\operatorname{lt}(\tau L) = \tau \operatorname{lt}(L)$ for every term τ and every nonzero operator $L \in K[\partial_1, \ldots, \partial_n]$. Moreover, it follows from the theory of Gröbner bases (discussed more deeply in the next section) that if I is an ideal, then a basis of the K-vector space $K[\partial_1, \ldots, \partial_n]/I$ is given by the equivalence classes of all terms τ that are not the leading term of an element of I. These observations give rise to the following general procedure for finding generators of an ideal.

Algorithm 4.73 *(FGLM)*
Input: *A term order and a method to determine the set of all K-linear combinations of a given finite set of terms* $\tau_1, \ldots, \tau_m$ *that belong to I, for a certain ideal* $I \subseteq K[\partial_1, \ldots, \partial_n]$.
Output: *An ideal basis of I and a K-vector space basis of* $K[\partial_1, \ldots, \partial_n]/I$.

1 *Set* $B = \emptyset$ *and* $G = \emptyset$.
2 *while there exist terms* $\partial_1^{e_1} \cdots \partial_n^{e_n}$ *which are not in B and not a multiple of some* $\operatorname{lt}(g)$ *for* $g \in G$ *do*
3   *Let* τ *be the smallest such term (with respect to the given term order).*
4   *Search for a nontrivial K-linear combination of* $B \cup \{\tau\}$ *that belongs to* I.
5   *if there is one then*
6   *Add this relation to G.*
7   *otherwise*
8   *Add* τ *to B.*
9 *Return G and* $\{\, [b] : b \in B \,\}$.

Example 4.74 Here is a possible trace of the algorithm. We choose the term order defined by $\partial_1^{u_1}\partial_2^{u_2} < \partial_1^{v_1}\partial_2^{v_2}$ if $u_1 < v_1 \vee (u_1 = v_1 \wedge u_2 < v_2)$. In the figures below, a term $\partial_1^{u_1}\partial_2^{u_2}$ corresponds to a point $(u_1, u_2) \in \mathbb{N}^2$. Terms in B are depicted as open circles, the term τ chosen in line 3 of the algorithm is depicted as a filled-in circle, and the terms in the shaded area are multiples of leading terms of elements of G. The nth figure ($n = 1, \ldots, 8$) shows the situation right after the nth execution of line 3. The last figure shows the situation when the while loop has terminated.



□

We have to explain why Algorithm 4.73 terminates and why its output is indeed an ideal basis. For the termination, we need to show that both branches of the if statement in lines 6 and 8 can only be executed a finite number of times. For the statement in line 8, this is easy to see when $K[\partial_1, \dots, \partial_n]/I$ is a finite dimensional K-vector space, because the equivalence classes of the elements of B are by construction always linearly independent over K. If the quotient $K[\partial_1, \dots, \partial_n]/I$ has infinite dimension, then the algorithm does not terminate. Regardless of whether the dimension of $K[\partial_1, \dots, \partial_n]/I$ is finite or not, the statement in line 6 can only be executed a finite number of times, although this is not totally obvious. The reason is the so-called *Dickson's lemma*, which says that every sequence $\tau_1, \tau_2, \tau_3, \dots$ of terms such that no term τ_i is a multiple of any of its predecessors $\tau_1, \dots, \tau_{i-1}$ must be finite. Note that this condition applies to the sequence of leading terms $\operatorname{lt}(g)$ added to G by the second part of the termination condition of the while loop.

Theorem 4.75 *Algorithm 4.73 is correct.* □

Proof We have to show that G is a basis of the ideal and that $\{\,[b] : b \in B\,\}$ is a vector space basis of the quotient.

It is clear that every element of G belongs to I, because only elements of I are added to G during the algorithm. It is also clear that $\{\,[b] : b \in B\,\}$ is linearly independent, because only terms are added to B that do not produce a linear dependence.

In order to show that G generates I and that $\{\,[b] : b \in B\,\}$ generates $K[\partial_1, \dots, \partial_n]/I$, we show that every element L of $K[\partial_1, \dots, \partial_n]$ is equivalent modulo $\langle G\rangle$ to a linear combination of elements of B. By the linear independence of B modulo I if and only if this linear combination is zero, this implies that L belongs to I. It also implies that B generates the quotient as a K-vector space, because any element of the quotient which was not in the (sub)space generated by the equivalence classes of elements of B would give rise to a counterexample.

Suppose the contrary, that there are elements of $K[\partial_1, \dots, \partial_n]$ that are not equivalent modulo $\langle G \rangle$ to a linear combination of elements of B, and among them, let L be one that is minimal in the sense that its largest term τ not contained in B is as small as possible with respect to the term order. By the termination condition of the while loop, any term not contained in B is a multiple of $\operatorname{lt}(g)$ for some $g \in G$. Therefore, there are $p \in K$, a term σ, and a $g \in G$ such that $L - p\sigma g$ does not contain τ. Since L is by assumption not equivalent modulo $\langle G \rangle$ to a linear combination of elements of B, and L is equivalent modulo $\langle G \rangle$ to $L - p\sigma g$, the operator $L - p\sigma g$ must still contain some term that is not in B. However, all such terms must be smaller than $\tau = \sigma \operatorname{lt}(g)$, in contradiction to the minimality assumption on L. ■

Exercises

1. Show that $\dim_{C(x,y)} C(x, y)[D_x, D_y]/\operatorname{ann}(x + \exp(x + y)) = 2$.

2*.** Show that x^n is D-finite and that $\log(n + x)$ is not.

3. For every $\alpha \in \mathbb{Q}$, determine a basis of the annihilator of $(x^3(x + y)y^2)^\alpha$ with respect to $C(x, y)[D_x, D_y]$.

4. In the proof of Theorem 4.69 we assumed that f belongs to the basis. What if $f = 0$?

5*.** Show that a sequence $(a_{k_1,\dots,k_n})_{k_1,\dots,k_n=0}^{\infty}$ is holonomic with respect to the algebra $C[k_1, \dots, k_n][S_{k_1}, \dots, S_{k_n}]$ if and only if its generating function

$$\sum_{k_1,\dots,k_n=0}^{\infty} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n} \in C[[x_1, \dots, x_n]]$$

is holonomic w.r.t. $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$.

Hint: First show that both statements are equivalent to holonomy of the generating function with respect to $C[x_1, \dots, x_n][\theta_{x_1}, \dots, \theta_{x_n}]$, where θ_{x_i} acts as the Euler derivation $x_i D_{x_i}$ $(i = 1, \dots, n)$.

6. The goal of this exercise is to show that a D-finite object depending on n variables can always be viewed as a D-finite object in $n + 1$ variables. To set things up, consider an Ore algebra $K[\partial_1, \ldots, \partial_n, \partial_{n+1}]$ and let F be a module for the subalgebra $K[\partial_1, \ldots, \partial_n]$.

a. Show that F becomes a $K[\partial_1, \ldots, \partial_n, \partial_{n+1}]$-module by defining $\partial_{n+1} \cdot f = 0$ for every $f \in F$.

b. Show that if $f \in F$ is D-finite with respect to $K[\partial_1, \ldots, \partial_n]$, it is also D-finite with respect to $K[\partial_1, \ldots, \partial_n, \partial_{n+1}]$.

7. Prove or disprove: If a sequence $(a_{n,k})_{n,k=0}^{\infty}$ is such that for every fixed $k \in \mathbb{N}$ the univariate sequence $(a_{n,k})_{n=0}^{\infty}$ is D-finite, then $(a_{n,k})_{n,k=0}^{\infty}$ is D-finite as a bivariate sequence.

8⋆. **a.** Let $r_1, \ldots, r_n \in C(x)$ be such that their denominators are pairwise coprime. Show that $r_1, \ldots, r_n$ are linearly independent over C.

b. Let $m \in \mathbb{Q} \setminus \mathbb{Z}$. Show that the polynomials $(m+u)^2 + (x+v)^2$ for $u, v \in \mathbb{Z}$ are pairwise coprime.

9. Prove or disprove: $1/(n^2 - k^2)$ is holonomic.

10⋆. Prove or disprove: $1/(nk+1)$ is holonomic.

11. Prove or disprove: If $I, J \subseteq C[x_1, \ldots, x_n, \partial_{x_1}, \ldots, \partial_{x_n}]$ are nontrivial (i.e., different from $\langle 1 \rangle$) and holonomic, then $I \subseteq J$ implies $I = J$.

12⋆⋆⋆. Show that $\sum_{k=1}^{n} \frac{1}{x+k}$ is not D-finite.

13. Show that the Legendre polynomials are holonomic in n and x. *Hint:* Guess and prove appropriate annihilating operators.

14. Let the linear functions $g_1, \ldots, g_n \colon \mathbb{Q}^m \to \mathbb{Q}$ be linearly independent over C. Show that $g_1, \ldots, g_n$ are algebraically independent.

15⋆. We have seen that if a multivariate sequence is D-finite, its generating function need not be D-finite. How about the converse: If a multivariate power series is D-finite, does its coefficient sequence have to be D-finite?

16⋆⋆. Let F be a $C(x, y)[D_x, D_y]$-module and $f \in F$.

a. Show that $\operatorname{ann}(f) = \langle D_x - x, D_y - x \rangle$ implies $f = 0$.

b. Suppose that there is an embedding $\phi\colon C(x, y)[D_x, D_y] \cdot f \to C(x, y)^2$ with the companion matrices $A_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $A_y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $f = 0$.

17⋆. Let $A = K[\partial_1, \ldots, \partial_n]$ be an Ore algebra, F be an A-module and let $m\colon F \times F \to F$ be a bilinear map. Let $f, g \in F$ be D-finite. Suppose there is an embedding $\phi\colon A \cdot f \to K^2$ with $\phi(f) = (1, 0) \in K^2$ and companion matrices $A_1, \ldots, A_n \in K^{2\times 2}$ and an embedding $\psi\colon A \cdot g \to K^2$ with $\psi(g) = (1, 0) \in K^2$ and companion matrices $B_1, \ldots, B_n \in K^{2\times 2}$. We want to construct an embedding $\chi\colon A \cdot m(f, g) \to K^4$ with $\chi(m(f, g)) = (1, 0, 0, 0)$. Find a companion matrix for the action of ∂_i

a. if $\partial_i \cdot m(a, b) = m(\partial_i \cdot a, \partial_i \cdot b)$ for all $a, b \in F$,

b. if $\partial_i \cdot m(a, b) = m(\partial_i \cdot a, b) + m(a, \partial_i \cdot b)$ for all $a, b \in F$.

18. Suppose that $f\colon \mathbb{Z}^2 \to C[[x, y]]$ is D-finite. Show that $f(3n + 5k, 2n - k, \sqrt{1 - xy}, x^2 + y^2)$ is D-finite as well.

19*. Let $u, v \in \mathbb{Q}^n$ and define $f\colon \mathbb{Z}^n \to C$ by

$$f(k_1, \dots, k_n) = \begin{cases} 1 \text{ if } \bigl((k_1, \dots, k_n) - u\bigr) \cdot v \geq 0, \\ 0 \text{ otherwise,} \end{cases}$$

so that f is 1 for the points in a certain halfspace defined by u and v, and 0 outside of this halfspace. Show that f is holonomic.

20. Let $I = \langle (1 - xy)D_x + y^2 D_y - y, (1 - xy)D_y^2 + x^2 y D_y - x^2 \rangle \subseteq C(x, y)[D_x, D_y]$. Construct an embedding $\phi\colon C(x, y)[D_x, D_y]/I \to C(x, y)^2$.

21. For a certain D-finite sequence f we have an embedding $\phi\colon C(n, k)[S_n, S_k] \cdot f \to C(n, k)^2$ with $\phi(f) = \binom{1}{1}$ and the companion matrices

$$A_n = \begin{pmatrix} \frac{2(n+1)(2n+1)}{(n+k+1)(n-k+1)} & 0 \\ 0 & 1 \end{pmatrix}, \quad A_k = \begin{pmatrix} \frac{n-k}{n+k+1} & 0 \\ 0 & 1 \end{pmatrix}$$

describing the action of S_n, S_k, respectively. Compute a basis of an ideal $I \subseteq C(n, k)[S_n, S_k]$ with $\dim_{C(n,k)} C(n, k)[S_n, S_k]/I = 2$ and $I \subseteq \operatorname{ann}(f)$. Can we tell whether $I = \operatorname{ann}(f)$?

22*. For the Legendre polynomials $P_n(x)$ we have $\operatorname{ann}(P_n(x)) = \langle (n + 1)S_n - (x^2 - 1)D_x - (n+1)x, (x^2 - 1)D_x^2 + 2xD_x - n(n+1) \rangle \subseteq C(n, x)[S_n, D_x]$. Compute an ideal basis of $\operatorname{ann}(P_n(x)^2)$.

23. Let $a(x, y)$ be an algebraic function satisfying the polynomial equation $a(x, y)^4 - xa(x, y)^2 + y = 0$. Find an ideal $I \subseteq C(x, y)[D_x, D_y]$ with $\operatorname{ann} a(x, y) \subseteq I$ and $\dim_{C(x,y)} C(x, y)[D_x, D_y]/I = 2$.

24. Show that the sum of two holonomic sequences is holonomic.

25*. Let $a(x, y) \in C[[x, y]]$ be D-finite and such that $a(x, y) = a(y, x)$.

a. Show that there are nonzero annihilating operators of $a(x, y)$ which are invariant under exchanging x with y and D_x with D_y.

b. Show that not all annihilating operators of $a(x, y)$ have this property.

26*. (Shaoshi Chen)

a. If $a \in C[[t]]$ is such that $a(xy) \in C[[x, y]]$ is D-finite, then a is D-finite in the sense of Chap. 3.

b. If $a \in C[[x, y]]$ is such that $(xD_x - yD_y)^s \cdot a = 0$ for some $s \in \mathbb{N}$, then there exists $b \in C[[t]]$ such that $a(x, y) = b(xy)$.

27.** Show that there is no algorithm which for any given

$$L \in C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$$

decides whether there exists a nonzero polynomial $p \in C[x_1, \dots, x_n]$ such that $L \cdot p = 0$.

Hint: You may use Matiyasevich's theorem, which says that there is no algorithm which for any given polynomial $p \in \mathbb{Z}[x_1, \dots, x_n]$ decides whether there is a tuple $(\xi_1, \dots, \xi_n) \in \mathbb{N}^n$ such that $p(\xi_1, \dots, \xi_n) = 0$.

References

Multivariate D-finite functions were first considered by Zeilberger [466]. He calls them multi-D-finite in the differential case and multi-P-recursive in the shift case. Ore algebras were first used to describe multivariate objects by Chyzak and Salvy [157]. They propose the notion *∂-finite* for what we call D-finite in Definition 4.67. Lipshitz [314] observed that generating functions of D-finite sequences need not be D-finite, which led Zeilberger to use holonomy instead of D-finiteness in his paper [468].

Holonomy was introduced by Bernstein [58] and has developed into a rather sophisticated theory [69, 166, 260, 377], of which we hardly make any use here. A fundamental result of the theory, known as Bernstein's inequality, is that for a proper left ideal $I \subsetneq C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$, it cannot happen that $I \cap C[U] \neq \{0\}$ for every subset $U \subseteq \{x_1, \dots, x_n, D_{x_1}, \dots, D_{x_n}\}$ with $|U| = n + 2$. Algebraically speaking, this means that the dimension of any proper left ideal of $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$ is at least n. In view of this result, a proper ideal is holonomic if it has smallest possible dimension. Another peculiar fact due to Stafford [307, 411] is that every left ideal of $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$ can be generated by only two elements.

We have seen in Sect. 2.2 that the dimension of the solution space of a linear recurrence with polynomial coefficients may exceed the order of the equation. The same is true in the multivariate case. Abramov and Petkovšek show that the solution space of a system of recurrences of first order can have any dimension [19].

Algorithm 4.73 is named after the initials of Faugère, Gianni, Lazard, and Mora, who propose this technique in [191] for changing the term order of a Gröbner basis. Essentially the same idea was already used a decade earlier by Buchberger and Möller for constructing Gröbner bases of ideals with finitely many solutions [118]. Dickson's lemma comes from [171].

4.6 Gröbner Bases

The annihilating operators of a D-finite object form a left ideal of the operator algebra. In the univariate case, the operator algebra is typically an Ore algebra of the form $K[\partial]$, which is a principal left ideal domain, so every ideal can be described by a single generator. It consists of all the left multiples of such a generator. In the case of several variables, an ideal is not necessarily generated by a single operator, but it remains true that every ideal can be described by a finite set of generators. This is Hilbert's basis theorem, which was originally formulated for commutative polynomial rings $C[x_1, \ldots, x_n]$ over a field but also holds for Ore algebras $K[\partial_1, \ldots, \partial_n]$.

If we are given a finite set $B \subseteq K[\partial_1, \ldots, \partial_n]$, it is not necessarily easy to answer questions about the left ideal $\langle B \rangle$ it generates. Even the answer to the question of whether or not the ideal contains 1 may not be obvious at first glance. Gröbner bases theory gives a finite set G of generators for an ideal $I \subseteq K[\partial_1, \ldots, \partial_n]$ such that many questions about I can be easily answered by looking at G. The theory is rich and has many applications, especially in the commutative case, for which it was first developed. There are several excellent textbooks exclusively devoted to Gröbner bases for commutative polynomial rings, and since the theory extends almost literally to the case of Ore algebras, we only give a minimal discussion here.

We are primarily interested in two kinds of noncommutative polynomial rings: Ore algebras $C(x_1, \ldots, x_m)[\partial_1, \ldots, \partial_k]$ in which $x_1, \ldots, x_m$ belong to the ground field, and Ore algebras $C[x_1, \ldots, x_m][\partial_1, \ldots, \partial_k]$ in which $x_1, \ldots, x_m$ are also considered as polynomial variables. In order to cover both cases with a common notation, let us write $K[X_1, \ldots, X_n]$ for the rings under consideration, where K may refer to either $C(x_1, \ldots, x_m)$ or C, and the variables $X_1, \ldots, X_n$ may refer either just to $\partial_1, \ldots, \partial_k$ or to $x_1, \ldots, x_m, \partial_1, \ldots, \partial_k$.

It remains true that every element of $K[X_1, \ldots, X_n]$ can be written as a (left-) K-linear combination of terms of the form $X_1^{e_1} \cdots X_n^{e_n}$ with $e_1, \ldots, e_n \in \mathbb{N}$, but we may no longer assume that the product of two terms is again a term. For example, in $C[x, y][D_x, D_y]$ we have $D_x x = x D_x + 1$. We therefore need to refine the definition of term orders used in the previous section. Like before, if $\leq$ is a total order on the set of all terms, we call the largest term with respect to $\leq$ appearing in an element $p \in K[X_1, \ldots, X_n] \setminus \{0\}$ the *leading term* of p and denote it by $\operatorname{lt}(p)$. We also define the *leading coefficient* $\operatorname{lc}(p) := [\operatorname{lt}(p)]p$ and the *leading monomial* $\operatorname{lm}(p) := \operatorname{lc}(p) \operatorname{lt}(p)$ of p. The *leading exponent* $\operatorname{lexp}(p)$ of p is defined as the vector $(e_1, \ldots, e_n)$ such that $\operatorname{lt}(p) = X_1^{e_1} \cdots X_n^{e_n}$. Note that all of these notions depend on the choice of the order $\leq$.

A total order $\leq$ on the set of terms is now called a *term order* (or *monomial order* or *admissible order*) if (i) $1 = X_1^0 \cdots X_n^0$ is the minimal element with respect to $\leq$; (ii) $\tau \leq \sigma \Rightarrow \operatorname{lt}(\rho\tau) \leq \operatorname{lt}(\rho\sigma)$ for all terms τ, σ, ρ; (iii) for all i, j with $i < j$ there exist $u \in K \setminus \{0\}$ and $v \in K[X_1, \ldots, X_n]$ with $v = 0$ or $\operatorname{lt}(v) < X_i X_j$ such that $X_j X_i = u X_i X_j + v$. This definition differs from the commutative case, where condition (iii) is not needed because it follows from (ii), and where on the right hand side of the implication in (ii) it suffices to say $\rho\tau \leq \rho\sigma$ because products of terms are terms. The adjustments are made in such a way that the rest of the theory carries over seamlessly to the present setting.

We assume from now on that the ring $K[X_1, \ldots, X_n]$ is endowed with a certain fixed term order $\leq$. Once a term order is fixed, we can perform division with remainder. In the commutative case, the algorithm for division with remainder is based on divisibility properties of leading terms. In $K[X_1, \ldots, X_n]$, we cannot easily say that one term is a divisor of another term because products of terms need not be terms. But we can talk about exponent vectors instead. For two vectors $(e_1, \ldots, e_n), (e'_1, \ldots, e'_n) \in \mathbb{N}^n$, we write $(e_1, \ldots, e_n) \leq (e'_1, \ldots, e'_n)$ if $\forall\, i : e_i \leq e'_i$. Then the divisibility $\operatorname{lt}(p) \mid \operatorname{lt}(q)$ used in the commutative case translates into the relation $\operatorname{lexp}(p) \leq \operatorname{lexp}(q)$. With this notation, the division algorithm can be formulated as follows.

Algorithm 4.76 *(Reduction)*
Input: $p \in K[X_1, \ldots, X_n]$, $G \subseteq K[X_1, \ldots, X_n]$, *a term order* $\leq$.
Output: $r \in K[X_1, \ldots, X_n]$ *such that* $p - r \in \langle G \rangle$ *and* r *contains no terms* τ *with* $\operatorname{lexp}(g) \leq \operatorname{lexp}(\tau)$ *for some* $g \in G$.

1 *Set* $r = 0$.
2 *while* $p \neq 0$ *do*
3 *if there is a* $g \in G$ *and a term* τ *in* p *such that* $\operatorname{lexp}(g) \leq \operatorname{lexp}(\tau)$ *then*
4 *Let* $g \in G$ *and* $\sigma = X_1^{e_1} \cdots X_n^{e_n}$ *be such that* $\operatorname{lt}(\sigma \operatorname{lc}(g)^{-1} g) = \tau$.
5 *Set* $p = p - ([\tau]p)\sigma \operatorname{lc}(g)^{-1} g$.
6 *else*
7 *Set* $p = p - ([\tau]p)\tau$ *and* $r = r + ([\tau]p)\tau$.
8 *Return* r.

It is easy to see that the algorithm is correct. Indeed, we obviously have $p - r \in \langle G \rangle$ in the beginning, and the property is preserved in every iteration of the loop, regardless of whether line 5 or line 7 is executed. So $p - r \in \langle G \rangle$ is true in the end. Moreoever, in line 7 we only introduce monomials into r whose exponent vectors are not above the leading exponent of any element of G, so this is also true at the end.

It is less clear that the algorithm terminates. Lines 5 and 7 are designed to cancel a term from p, but line 5 may introduce many other terms, which will be smaller in term order than the eliminated term. From a hypothetical infinite run of the algorithm, it can be deduced that there is an infinite strictly descending sequence of terms. Since such a sequence does not exist by Dickson's lemma, the algorithm terminates.

It is also not clear why the output of the algorithm is independent of the choice of g made in line 4, if there are several options. In fact, no claim is made that the output is unique, and in general, different choices of g in line 4 do lead to different output. A starting point of the theory of Gröbner bases is the desire to make the output unique by imposing appropriate restrictions on G. In view of this goal, let us use the notation $\operatorname{red}(p, G)$ for any possible outcome of Algorithm 4.76 when applied to $p \in K[X_1, \ldots, X_n]$ and $G \subseteq K[X_1, \ldots, X_n]$. Note that in view of the non-uniqueness, $\operatorname{red}(\cdot, G)$ is not a function, and $\operatorname{red}(p, G) = r_1$ and $\operatorname{red}(p, G) = r_2$ does not imply $r_1 = r_2$. This is similar to the big-O notation. If the term order is not clear from context, we write $\operatorname{red}_{\leq}(p, G)$ instead of $\operatorname{red}(p, G)$.

The definition of Gröbner bases is motivated by the following theorem.

Theorem 4.77 *Let* $G \subseteq K[X_1, \ldots, X_n]$. *Then the following are equivalent:*

1. *For all* $p \in K[X_1, \ldots, X_n]$ *there exists exactly one* $r \in K[X_1, \ldots, X_n]$ *with* $\operatorname{red}(p, G) = r$.
2. *For all* $p \in \langle G \rangle$ *we have* $\operatorname{red}(p, G) = 0$.
3. *For all* $p \in \langle G \rangle \setminus \{0\}$ *there exists a* $g \in G$ *with* $\operatorname{lexp}(g) \leq \operatorname{lexp}(p)$.
4. *The set of all equivalence classes of terms* $\tau = X_1^{e_1} \cdots X_n^{e_n}$ *with* $\operatorname{red}(\tau, G) = \tau$ *forms a* K*-vector space basis of* $K[X_1, \ldots, X_n]/\langle G \rangle$. □

Proof 1. ⇒ 2.: Let $p \in \langle G \rangle$ and let $r = \operatorname{red}(p, G)$. We have to show that $r = 0$.

First observe that for every $u \in K[X_1, \ldots, X_n]$, every $c \in K$, every term $\tau = X_1^{e_1} \cdots X_n^{e_n}$, and every $g \in G$ we have $\operatorname{red}(u + c\tau \operatorname{lc}(g)^{-1} g, G) = \operatorname{red}(u, G)$. This is a consequence of assuming 1. (See Exercise 7 for a detailed argument.)

Since $p \in \langle G \rangle$, there is a way to write $p = \sum_{i=1}^m c_i \tau_i \operatorname{lc}(g_i)^{-1} g_i$ with certain ground field elements $c_i \in K$, certain terms τ_i, and certain elements g_i of G (not necessarily pairwise distinct). Applying the observation m times, we find that $0 = \operatorname{red}(0, G) = \operatorname{red}(p - \sum_{i=1}^m c_i \tau_i \operatorname{lc}(g_i)^{-1} g_i, G) = r$, as required.

2. ⇒ 3.: If $p \neq 0$ reduces to zero, the reduction process must have at least one step. The reduction process as formulated in Algorithm 4.76 is not forced to start with eliminating the leading term of p, but as long as it keeps eliminating smaller terms, the leading term of p will remain unchanged. In order to eventually reach zero, it must at some point choose a g with $\operatorname{lexp}(g) \leq \operatorname{lexp}(p)$ in order to also eliminate the leading term. Therefore, such a g must exist.

3. ⇒ 4.: Let B be the set of equivalence classes defined in the statement. It is clear that B generates $K[X_1, \ldots, X_n]/\langle G \rangle$ because for every $p \in K[X_1, \ldots, X_n]$ we have $[p] = [\operatorname{red}(p, G)]$ and $\operatorname{red}(p, G)$ only contains terms τ with $\operatorname{red}(\tau, G) = \tau$, so $[p]$ is a K-linear combination of elements of B. The set B is also K-linearly independent, for if $[p]$ is a K-linear combination of elements of B, we may assume that p is a K-linear combination of terms τ with $\operatorname{red}(\tau, G) = \tau$. The class $[p]$ is zero if and only if $p \in \langle G \rangle$, which by assumption implies $\operatorname{red}(p, G) = 0$. But since p does not contain any terms that can be reduced, it cannot contain any terms at all. From $p = 0$ follows the linear independence of B.

4. ⇒ 1.: Let $p \in K[X_1, \ldots, X_n]$ and let $r_1, r_2 \in K[X_1, \ldots, X_n]$ be such that $\operatorname{red}(p, G) = r_1$ and $\operatorname{red}(p, G) = r_2$. Then r_1 and r_2 contain only terms τ with $\operatorname{red}(\tau, G) = \tau$. Moreover, $r_1 - r_2$ is an element of the ideal, so $[r_1 - r_2] = 0$. Since the set B in statement 4 is linearly independent by assumption, it follows that $r_1 = r_2$. ■

Definition 4.78 A set $G \subseteq K[X_1, \ldots, X_n]$ is called a *Gröbner basis* (of the left ideal $\langle G \rangle$) if it satisfies any of the equivalent conditions of Theorem 4.77. □

Every left ideal I of $K[X_1, \ldots, X_n]$ is a Gröbner basis (of itself). The reason is that every $p \in I$ can be reduced to zero in one step. It is also not hard to see that for every left ideal I of $K[X_1, \ldots, X_n]$, there exists a finite Gröbner basis G with $\langle G \rangle = I$. The reason is Dickson's lemma: start with an arbitrary element $g_1 \in I \setminus \{0\}$, then, if possible, choose an element $g_2 \in I \setminus \{0\}$ with $\operatorname{red}(\operatorname{lt}(g_2), \{g_1\}) = \operatorname{lt}(g_2)$, then, if possible, an element $g_3 \in I$ with $\operatorname{red}(\operatorname{lt}(g_3), \{g_1, g_2\}) = \operatorname{lt}(g_3)$, and so on. Because of $\operatorname{lexp}(g_1) > \operatorname{lexp}(g_2) > \operatorname{lexp}(g_3) > \cdots$, the process must come to an end after finitely many steps. The resulting set $\{g_1, \ldots, g_k\}$ is the desired Gröbner basis.

This argument is not constructive. If we want to compute a Gröbner basis for a given ideal I, we first have to agree what it means for I to be "given". One situation is that we know some finite set $B \subseteq K[X_1, \ldots, X_n]$ such that $I = \langle B \rangle$ and want to know a Gröbner basis G with $I = \langle G \rangle$. This problem is solved by Buchberger's algorithm, which is explained below. Another typical situation is if we can apply Algorithm 4.73 with our knowledge about I. Observe that the ideal basis returned by Algorithm 4.73 is always a Gröbner basis, which can be seen using characterization 4 of Theorem 4.77.

Knowing a Gröbner basis, we can also meet the input requirements of Algorithm 4.73. Namely, in order to find K-linear combinations modulo $\langle G \rangle$ among some given terms $\tau_1, \ldots, \tau_m$, we can make an ansatz $u_1\tau_1 + \cdots + u_m\tau_m$ for undetermined $u_i \in K$ and force $\operatorname{red}(u_1\tau_1 + \cdots + u_m\tau_m, G) = u_1 \operatorname{red}(\tau_1, G) + \cdots + u_m \operatorname{red}(\tau_m, G) = 0$ by equating coefficients of like terms. But why would we want to compute a Gröbner basis if we already have one? One reason could be that we only know a Gröbner basis with respect to a certain term order $\leq_1$ but we would need a Gröbner basis for the same ideal with respect to some other term order $\leq_2$. Another situation is when we know a Gröbner basis for some ideal(s) but would like to compute a (Gröbner) basis for a different ideal. For example, suppose we already know Gröbner bases G_1, G_2 of $\operatorname{ann}(f_1)$ and $\operatorname{ann}(f_2)$ for two D-finite functions f_1 and f_2. Then $\operatorname{ann}(f_1) \cap \operatorname{ann}(f_2)$ is an ideal of annihilating operators for $f_1 + f_2$, and we can use Algorithm 4.73 to compute generators for it. As input to the algorithm, we can use a procedure which for given terms $\tau_1, \ldots, \tau_m$ computes $u_1, \ldots, u_m \in K$ such that $u_1 \operatorname{red}(\tau_1, G_1) + \cdots + u_m \operatorname{red}(\tau_m, G_1) = 0$ and $u_1 \operatorname{red}(\tau_1, G_2) + \cdots + u_m \operatorname{red}(\tau_m, G_2) = 0$. Other closure properties can be executed in a similar fashion.

Of particular interest in the context of D-finite functions is characterization 4 of Theorem 4.77. Suppose we have a function f for which we know a Gröbner basis G of the ideal $\operatorname{ann}(f) \subseteq K[\partial_1, \ldots, \partial_n]$. By Definition 4.63, f is D-finite if and only if $\dim_K K[\partial_1, \ldots, \partial_n]/\operatorname{ann}(f) < \infty$. According to Exercise 9, this is the case if and only if for every $i \in \{1, \ldots, n\}$ there exists a $g \in G$ whose leading term is a power of ∂_i, a condition that can easily be checked by inspection. Gröbner bases can also be used for checking whether an ideal is holonomic. Suppose we know a basis B of the ideal $I \subseteq C[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$. According to Definition 4.67, I is holonomic if and only if $I \cap C[U] \neq \{0\}$ for every $U \subseteq \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$ with $|U| = n + 1$. For each such U, select a term order for which terms consisting only of variables from U are smaller than terms containing other variables. Such a term order is called an *elimination order* (for U). It follows easily from the defining properties of Theorem 4.77 that the ideal $I \cap C[U]$ is generated by $G \cap C[U]$ whenever G is a Gröbner basis with respect to an elimination order for U. In particular, $I \cap C[U] \neq \{0\}$ if and only if $G \cap C[U] \neq \emptyset$.

For computing a Gröbner basis from an arbitrary (but finite) given ideal basis, none of the conditions of Theorem 4.77 are particularly useful, because all are statements about infinitely many cases that cannot simply be checked one by one.

Buchberger's algorithm is based on a different characterization which only affects finitely many cases. In the commutative case, the *S-polynomial* of two polynomials $p, q \in C[x_1, \ldots, x_n] \setminus \{0\}$ is defined as

$$\operatorname{spol}(p, q) = \frac{\operatorname{lcm}(\operatorname{lt}(p), \operatorname{lt}(q))}{\operatorname{lm}(p)} p - \frac{\operatorname{lcm}(\operatorname{lt}(p), \operatorname{lt}(q))}{\operatorname{lm}(q)} q.$$

In a sense, this is the smallest possible linear combination of p and q which induces a cancellation of the leading monomials of p and q. Note that both summands on the right have the leading term $\operatorname{lcm}(\operatorname{lt}(p), \operatorname{lt}(q))$. The same idea is used in the non-commutative case, but we should adapt the notation a bit, because speaking of the "least common multiple" of terms does not seem appropriate if the product of two terms is not necessarily again a term. It is safer to talk about exponent vectors. For two vectors $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$, define $\max(u, v) = (\max(u_1, v_1), \ldots, \max(u_n, v_n))$ and write X^u for $X_1^{u_1} \cdots X_n^{u_n}$. Then the *S-polynomial* of $p, q \in K[X_1, \ldots, X_n] \setminus \{0\}$ is defined as

$$\begin{aligned}\operatorname{spol}(p, q) = {} & X^{\max(\operatorname{lexp}(p), \operatorname{lexp}(q)) - \operatorname{lexp}(p)} \operatorname{lc}(p)^{-1} p \\ & - X^{\max(\operatorname{lexp}(p), \operatorname{lexp}(q)) - \operatorname{lexp}(q)} \operatorname{lc}(q)^{-1} q.\end{aligned}$$

Again, this is the smallest possible way to let the leading monomials of p and q cancel. With this definition of S-polynomials, Buchberger's characterization of Gröbner bases and his algorithm for computing Gröbner bases carry over literally from the commutative case.

Theorem 4.79 *A set $G \subseteq K[X_1, \ldots, X_n]$ is a Gröbner basis if and only if* $\operatorname{red}(\operatorname{spol}(p, q), G) = 0$ *for all $p, q \in G$.* □

Proof The direction "⇒" follows directly from Definition 4.78. To show "⇐", let $p \in \langle G \rangle$ be such that $\operatorname{red}(p, G) = p$, i.e., no term appearing in p can be matched with the leading term of a multiple of an element of G. We show that $p = 0$.

Since $p \in \langle G \rangle$, there are $g_1, \ldots, g_m \in G$ and $p_1, \ldots, p_m \in K[X_1, \ldots, X_n]$ such that $p = p_1 g_1 + \cdots + p_m g_m$. Since p cannot be reduced, the leading terms $\operatorname{lt}(p_i g_i)$ do not occur in p, so there must be some cancellation on the right hand side. We show that in fact the entire right hand side cancels.

Suppose otherwise. Let $\tau_i = \operatorname{lt}(p_i g_i)$ for $i = 1, \ldots, m$ and assume without loss of generality that the indexing is such that $\tau_1 \geq \tau_2 \geq \cdots \geq \tau_m$. We may further assume, also without loss of generality, that the coefficients $p_1, \ldots, p_m$ are chosen in such a way that τ_1 is as small as possible.

In view of the required cancellation, we must have $\tau_1 = \tau_2 = \cdots = \tau_k > \tau_{k+1}$ for some $k \geq 2$. We may further assume, again without loss of generality, that among all possible choices $p_1, \ldots, p_m$ that yield the minimal τ_1, our choice is made such that k is minimal.

We have

$$\operatorname{lm}(p_k)g_k = \operatorname{lm}(p_k)\operatorname{lc}(g_k)\operatorname{lc}(g_k)^{-1}g_k = (u\operatorname{lt}(p_k) + v)\operatorname{lc}(g_k)^{-1}g_k$$

for some $u \in K$ and some $v \in K[X_1, \dots, X_n]$ with $v = 0$ or $\operatorname{lt}(v) < \operatorname{lt}(p_k)$. There are also terms σ, μ such that

$$\operatorname{lt}(p_k)\operatorname{lc}(g_k)^{-1}g_k - \sigma\operatorname{lc}(g_{k-1})^{-1}g_{k-1} = \mu\operatorname{spol}(g_k, g_{k-1}).$$

Since $\operatorname{red}(\operatorname{spol}(g_k, g_{k-1}), G) = 0$ by assumption, there exist polynomials $q_1, \dots, q_m$ with

$$u\mu\operatorname{spol}(g_k, g_{k-1}) = q_1g_1 + \cdots + q_mg_m$$

and $\operatorname{lt}(q_ig_i) < \mu X^{\max(\operatorname{lexp}(g_k), \operatorname{lexp}(g_{k-1}))} = \tau_1$ for $i = 1, \dots, m$. Using $\operatorname{lm}(p_k) - v\operatorname{lc}(g_k)^{-1} = u\operatorname{lt}(p_k)\operatorname{lt}(g_k)^{-1}$, we get

$$\begin{aligned}
p = {} & \big(p_1 && + q_1 \big)g_1 \\
& \vdots \\
+ {} & \big(p_{k-2} && + q_{k-2}\big)g_{k-2} \\
+ {} & \big(p_{k-1} + u\sigma\operatorname{lc}(g_{k-1})^{-1} && + q_{k-1}\big)g_{k-1} \\
+ {} & \big(p_k \quad - (\operatorname{lm}(p_k) - v\operatorname{lc}(g_k)^{-1}) && + q_k \big)g_k \\
+ {} & \big(p_{k+1} && + q_{k+1}\big)g_{k+1} \\
& \vdots \\
+ {} & \big(p_m \underbrace{\qquad\qquad\qquad\qquad\qquad\qquad + q_m}_{=0} \big)g_m.
\end{aligned}$$

This new representation of p violates the minimality assumption on k, or, if $k = 2$, the minimality assumption of τ_1. ∎

Algorithm 4.80 *(Buchberger)*
Input: *A finite set $B \subseteq K[X_1, \dots, X_n] \setminus \{0\}$ and a term order $\leq$.*
Output: *A finite Gröbner basis $G \subseteq K[X_1, \dots, X_n]$ with respect to $\leq$ such that $\langle B\rangle = \langle G\rangle$.*

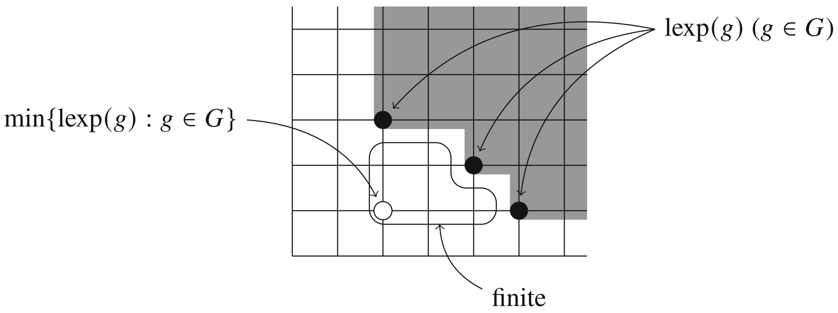
Set $G = B = \{b_1, \dots, b_m\}$.
Set $P = \{(b_i, b_j) : 1 \leq i < j \leq m\}$.
while $P \neq \emptyset$ do
  Choose a pair $(p, q) \in P$ and set $P = P \setminus \{(p, q)\}$.
  Compute $h = \operatorname{red}(\operatorname{spol}(p, q), G)$.
  if $h \neq 0$ then

7 *Set* $P = P \cup \{(p, h) : p \in G\}$ *and* $G = G \cup \{h\}$.
8 *Return* G.

Theorem 4.81 *Algorithm 4.80 is correct and terminates.* □

Proof Correctness follows from Theorem 4.79, because the algorithm terminates if G is such that all S-polynomials reduce to zero. Whenever the algorithm encounters an S-polynomial that does not reduce to zero, it adds the remainder h to G, so that h can then be reduced further to zero in one step. Recall that the notation $\operatorname{red}(\cdot, G)$ refers to any possible output of the reduction procedure and is not unique as long as G is not a Gröbner basis. However, if there is some way to reduce a certain S-polynomial $\operatorname{spol}(p, q)$ to zero at a given stage of the algorithm, then this feature is not harmed if we add further elements to G later during the computation. Therefore, when G gets updated, it is not necessary to reconsider the S-polynomials that have been handled up to that point.

For the termination, it suffices to show that line 7 cannot be executed infinitely often. At every execution of line 7, consider the vector $\min\{\operatorname{lexp}(g) : g \in G\} \in \mathbb{N}^n$. Since h cannot be reduced any further by G, we have $\operatorname{lexp}(g) \not\leq \operatorname{lexp}(h)$ for all $g \in G$. This does not necessarily mean that adding h to G leads to a drop in one of the coordinates of $\min\{\operatorname{lexp}(g) : g \in G\}$, but since there are only finitely many points above $\min\{\operatorname{lexp}(g) : g \in G\}$ and below the $\operatorname{lexp}(g)$ $(g \in G)$, the vector can cease to change only finitely many times. Hence, at least every now and then during a long execution, we must observe that at least one coordinate of $\min\{\operatorname{lexp}(g) : g \in G\}$ strictly decreases. Since no coordinate of the vector can ever increase, we must reach $(0, \ldots, 0)$ after finitely many steps, unless the algorithm terminates before. At this point, it terminates in any case. ■



Example 4.82 Consider the ideal $I = \langle b_1, b_2, b_3 \rangle \subseteq C(n, k)[S_n, S_k]$ with

$$b_1 = S_n^2 S_k + S_n S_k^2 - 3 S_n S_k - S_n - S_k^2 + S_k + 2,$$

$$b_2 = 5(k - n - 2) S_n^2 - (2n - 7) S_n S_k - (9k - 14n - 19) S_n$$
$$+ (k + 2) S_k^2 + (2k + n - 5) S_k + k - 8n - 16,$$

$$\begin{aligned} b_3 &= (5k-3n-2)S_nS_k - (k-n-1)S_n - (k+2)S_k^2 \\ &\quad - (2k-4n-5)S_k - k - 2n + 1. \end{aligned}$$

We want to compute a Gröbner basis with respect to the term order $\leq$ defined by $S_n^a S_k^b \leq S_n^u S_k^v$ if $a < u$ or $a = u$ and $b \leq v$. The terms in b_1, b_2, b_3 are already sorted according to this order.

We set $P = \{(b_1, b_2), (b_1, b_3), (b_2, b_3)\}$ and select (b_1, b_2) as the first pair. Its S-polynomial has the form

$$\begin{aligned} b_1 - S_k \tfrac{1}{5(k-n-2)} b_2 &= (\dots)S_n^2 + (\dots)S_nS_k^2 + (\dots)S_nS_k + (\dots)S_n \\ &\quad + (\dots)S_k^3 + (\dots)S_k^2 + (\dots)S_k + (\dots), \end{aligned}$$

where the $\dots$ are certain elements of $C(n,k)$ that we suppress here. Using Algorithm 4.76, the S-polynomial can be reduced to an operator of the form

$$(\dots)S_n + (\dots)S_k^3 + (\dots)S_k^2 + (\dots)S_k + (\dots).$$

As it is nonzero, we call it b_4 and add it to the basis. We also add the pairs (b_1, b_4), (b_2, b_4), (b_3, b_4) to P.

For the next pair, (b_1, b_3), the reduction of the S-polynomial produces an operator of the form

$$(\dots)S_k^3 + (\dots)S_k^2 + (\dots)S_k + (\dots),$$

and since it is nonzero, we call it b_5 and add it to the basis. We also add the pairs (b_1, b_5), (b_2, b_5), (b_3, b_5), (b_4, b_5) to P.

For the next pair, (b_2, b_3), the S-polynomial reduces to zero, so we get nothing new.

Next, (b_1, b_4) has an S-polynomial which reduces to an operator of the form

$$(\dots)S_k^2 + (\cdots)S_k + (\cdots),$$

which we add as b_6 to the basis. We also add the pairs $(b_1, b_6), \dots, (b_5, b_6)$ to P.

At this point, P contains 12 pairs, but it turns out that all corresponding S-polynomials reduce to zero, so we are done. The resulting Gröbner basis is $\{b_1, \dots, b_6\}$. □

Algorithm 4.80 is not explicit about how to make the choice of $(p, q) \in P$ in line 4. Indeed, a different choice can lead to a different output. Every ideal I of $K[X_1, \dots, X_n]$ has many different Gröbner bases (even for a fixed term order), and the only assertion about Algorithm 4.80 is that it will find one of them. We can eliminate this redundancy by imposing further constraints. A Gröbner basis G is called *reduced* if its elements are monic and we have $\operatorname{red}(g, G \setminus \{g\}) = g$ for all $g \in G$. It can be shown like in the commutative case that every ideal has exactly one reduced Gröbner basis (for a prescribed term order). Starting from any finite Gröbner basis, e.g., some output of Algorithm 4.80, we can find the reduced Gröbner basis by first replacing every element g by $\mathrm{red}(g, G \setminus \{g\})$ and afterwards dividing every element from the left by its leading coefficient.

While the choices made in line 4 are irrelevant for the correctness and termination of the algorithm, they can have a strong influence on the runtime. Many people have thought about these choices, and have proposed several *selection strategies*. Common strategies select the next pair (p, q) based on $\max(\mathrm{lexp}(p), \mathrm{lexp}(q))$ (preferring lower ones), on the age (preferring older ones), or on the number of terms (preferring smaller ones). More sophisticated strategies compute a certain score for each pair in P and select the pair with the highest score. Another way to improve the performance is to identify *useless pairs*. There are certain criteria by which it is possible to detect at low cost whether a given pair $(p, q) \in P$ can be discarded without harming the correctness. Some of the criteria known from the commutative theory carry over to the noncommutative setting (Exercise 17), others don't (Exercise 16).

Yet another way to improve the performance is to handle several pairs at the same time. Instead of a single pair (p, q) in line 4, we can select a subset $S \subseteq P$ with $|S| \geq 1$ and set $P = P \setminus S$. In a preprocessing step, we then determine all the term-multiples of elements of B that may occur during the reduction of S-polynomials of the selected pairs. By a term-multiple we mean an operator of the form τb with τ being a term and $b \in B$. These term-multiples can be found by doing a "dry-run" of the reduction algorithm with coefficients replaced by Booleans that signal the potential nonzeroness of a coefficient. When a suitable collection of term-multiples has been constructed, we can determine all terms appearing in these term-multiples or the S-polynomials of the selected pairs. We then set up a matrix in which the columns are labeled by these terms, in decreasing order from left to right, and with two rows per selected pair and one row for each determined term-multiple. For each pair (p, q), we fill the row for p with the coefficients of $X^{\max(\mathrm{lexp}(p),\mathrm{lexp}(q))-\mathrm{lexp}(p)}\,\mathrm{lc}(p)^{-1}p$ and the row for q with the coefficients of $X^{\max(\mathrm{lexp}(p),\mathrm{lexp}(q))-\mathrm{lexp}(q)}\,\mathrm{lc}(q)^{-1}q$. For each term-multiple, we put its coefficients into the corresponding row. The resulting matrix is then brought into echelon form using Gaussian elimination, and we select all rows whose left-most nonzero entry is in a column that corresponds to a term which cannot be reduced by any element of B. There may be zero, one, or several such rows. For each of them, let h be the element of $K[X_1, \ldots, X_n]$ whose coefficient vector is the row and execute line 7 of Algorithm 4.80. Then continue with a new selection $S \subseteq P$ and repeat the procedure until $P = \emptyset$.

Example 4.83 Considering the same input as in the previous example, let us take as S the whole initial set $P = \{(b_1, b_2), (b_1, b_3), (b_2, b_3)\}$. The three S-polynomials corresponding to these pairs are differences of b_1, $S_k\,\mathrm{lc}(b_2)^{-1}b_2$, and $S_n\,\mathrm{lc}(b_3)^{-1}b_3$, and the terms occurring in these operators are $S_n^2 S_k$, S_n^2, $S_n S_k^2$, $S_n S_k$, S_n, S_k^3, S_k^2, S_k, 1. For reducing polynomials involving these terms, we determine multiples of b_1, b_2, b_3 whose leading terms appear in this list.

They are $S_k b_3$ (with leading term $S_n S_k^2$), and b_1, b_2, b_3 themselves. These operators contain only terms that are already in the list, so we can form the matrix

$$\begin{array}{rc} & \begin{array}{ccccccccc} S_n^2 S_k & S_n^2 & S_n S_k^2 & S_n S_k & S_n & S_k^3 & S_k^2 & S_k & 1 \end{array} \\ \begin{array}{r} b_1 \\ S_k\,\mathrm{lc}(b_2)^{-1} b_2 \\ S_n\,\mathrm{lc}(b_3)^{-1} b_3 \\ S_k b_3 \\ b_2 \\ b_3 \end{array} & \begin{pmatrix} * & 0 & * & * & * & 0 & * & * & * \\ * & 0 & * & * & 0 & * & * & * & 0 \\ * & * & * & * & * & 0 & 0 & 0 & 0 \\ 0 & 0 & * & * & 0 & * & * & * & 0 \\ 0 & * & 0 & * & * & 0 & * & * & * \\ 0 & 0 & 0 & * & * & 0 & * & * & * \end{pmatrix} \end{array}.$$

Row reduction turns this matrix into

$$\begin{array}{rc} & \begin{array}{ccccccccc} S_n^2 S_k & S_n^2 & S_n S_k^2 & S_n S_k & S_n & S_k^3 & S_k^2 & S_k & 1 \end{array} \\ \begin{array}{r} \\ \\ \\ \\ \to \\ \to \end{array} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 1 & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & 1 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 1 & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & * \end{pmatrix} \end{array},$$

which has two rows (indicated by the arrows) that correspond to operators with new leading terms. The new leading terms are S_n and S_k^3, respectively, like for the operators b_4 and b_5 we found in the previous example. □

The theory of Gröbner bases can be generalized from ideals of $K[X_1, \dots, X_n]$ to submodules of $K[X_1, \dots, X_n]^d$. Elements of $K[X_1, \dots, X_n]^d$ are K-linear combinations of module terms, a module term being an element of the form $X_1^{u_1} \cdots X_n^{u_n} e_i$ with $u_1, \dots, u_n \in \mathbb{N}$ and e_i the ith unit vector. Term orders, reduction, the notion of Gröbner bases, and Buchberger's algorithm extend literally if we simply regard the unit vectors $e_1, \dots, e_d$ as additional variables subject to the constraints $e_i e_j = 0$ for $i, j = 1, \dots, d$. Of particular interest are term orders which first compare the index of the unit vector and then use a term order for the polynomials $X_1, \dots, X_n$ for breaking ties. Such a term order is called a POT order (position over term), as opposed to a TOP order (term over position) which first looks at $X_1, \dots, X_n$ and then uses the index of the unit vector to break ties.

One application of Gröbner bases for modules is the computation of syzygies and cofactors. A *syzygy* of $b_1, \dots, b_m \in K[X_1, \dots, X_m]$ is a vector $(p_1, \dots, p_m) \in K[X_1, \dots, X_n]^m$ with $p_1 b_1 + \cdots + p_m b_m = 0$. The set of all syzygies for a fixed choice of $b_1, \dots, b_m$ forms a (left-)submodule of $K[X_1, \dots, X_n]^m$, denoted by $\mathrm{Syz}(b_1, \dots, b_m)$. Cofactors are the coefficients which are used in order to express an ideal element in terms of generators of an ideal: $f \in \langle b_1, \dots, b_m \rangle$ means that there are $q_1, \dots, q_m \in K[X_1, \dots, X_n]$ with $f = q_1 b_1 + \cdots + q_m b_m$, and these $q_1, \dots, q_m$ are called *cofactors* of f with respect to $b_1, \dots, b_m$. They are in general not unique, but any two vectors of cofactors differ by a syzygy.

If $\{b_1, \ldots, b_m\}$ is a Gröbner basis, we can easily compute cofactors for any given $f \in \langle b_1, \ldots, b_m\rangle$ by an extended version of the reduction algorithm (Exercise 6). If it is not, we can compute a Gröbner basis $\{g_1, \ldots, g_k\}$ using Buchberger's algorithm. It is then easy to compute cofactors with respect to $g_1, \ldots, g_k$, but if we want cofactors with respect to the original basis, then we need to know how the elements of the Gröbner basis can be expressed in terms of the original basis elements. This information can be obtained by computing a Gröbner basis with respect to a POT order of the submodule generated by

$$\begin{pmatrix} b_1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} b_2 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} b_m \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

The Gröbner basis will have the form

$$\begin{pmatrix} g_1 \\ q_{1,1} \\ q_{2,1} \\ \vdots \\ q_{m,1} \end{pmatrix}, \ldots, \begin{pmatrix} g_k \\ q_{1,k} \\ q_{2,k} \\ \vdots \\ q_{m,k} \end{pmatrix}, \begin{pmatrix} 0 \\ p_{1,1} \\ p_{2,1} \\ \vdots \\ p_{m,1} \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ p_{1,\ell} \\ p_{2,\ell} \\ \vdots \\ p_{m,\ell} \end{pmatrix},$$

where $\{g_1, \ldots, g_k\}$ is a Gröbner basis of $\langle b_1, \ldots, b_m\rangle$ and the matrix $((q_{i,j}))_{i=1,j=1}^{m,k} \in K[X_1, \ldots, X_n]$ is the basis change matrix that translates linear combinations of $g_1, \ldots, g_k$ into linear combinations of $b_1, \ldots, b_m$. Moreover, the vectors

$$(p_{1,j}, \ldots, p_{m,j}) \in K[X_1, \ldots, X_n]^m$$

form a basis of the syzygy module of $b_1, \ldots, b_m$.

With the help of the syzygy module, we can make the intersection of ideals constructive. Given two ideals $I = \langle b_1, \ldots, b_m\rangle$, $J = \langle d_1, \ldots, d_k\rangle$, an operator belongs to the intersection $I \cap J$ if and only if it can be written as a linear combination of the b_i and as a linear combination of the d_j. The search for operators $p_1, \ldots, p_m$ and $q_1, \ldots, q_k$ with $p_1b_1 + \cdots + p_mb_m = q_1d_1 + \cdots + q_kd_k$ is the same as the search for the syzygy module of $b_1, \ldots, b_m, -d_1, \ldots, -d_k$. Once we have a basis of the syzygy module, we can take the first m coordinates of each basis element and combine them with $b_1, \ldots, b_m$. The resulting operators are generators of the intersection ideal. This approach generalizes the idea of Exercise 14 in Sect. 4.2 to the case of several variables and provides an alternative way to compute an annihilating ideal for the sum of two D-finite objects from given annihilating ideals of the summands.

Gröbner bases for modules can also be used to uncouple systems of operator equations. Given a system $A \cdot f = 0$ with a known $A \in K[\partial]^{r \times r}$ and an unknown $f \in F^r$, we can consider the module generated in $K[\partial]^r$ by the rows of A. Computing a Gröbner basis of this module with respect to a POT order is equivalent to computing a Hermite normal form of A.

Exercises

1. Show that Hilbert's basis theorem, which says that every ideal of an Ore algebra $K[X_1, \ldots, X_n]$ has a finite basis, is equivalent to the ascending chain condition, which says that for every chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals of $K[X_1, \ldots, X_n]$ there exists an $m \in \mathbb{N}$ such that $I_m = I_{m+1} = \cdots$.

2. Let $\leq$ be a term order for the commutative polynomial ring $C[x_1, \ldots, x_n]$. Consider an Ore algebra $K[\partial_1, \ldots, \partial_n]$. Show that $\leq$ is also a valid term order for $K[\partial_1, \ldots, \partial_n]$ if we set $\partial_1^{u_1} \cdots \partial_n^{u_n} \leq \partial_1^{v_1} \cdots \partial_n^{v_n} \iff x_1^{u_1} \cdots x_n^{u_n} \leq x_1^{v_1} \cdots x_n^{v_n}$.

3. Let $\leq$ be a term order for the commutative ring $C[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
a. Show that $\leq$ is also a valid term order for $C[x_1, \ldots, x_n, D_1, \ldots, D_n]$ (with the D_i being compared like the y_i).
b. Show that $\leq$ is also a valid term order for $C[x_1, \ldots, x_n, S_1, \ldots, S_n]$ (with the S_i being compared like the y_i).

4. Consider the Ore algebra $C[x, M_5]$ with the commutation rule $M_5 x = x^5 M_5$. Show that there is no term order for $C[x, M_5]$.

5. Show by an example that condition (iii) in the definition of term orders does not follow from conditions (i) and (ii) in general.

6. Extend Algorithm 4.76 so that it returns not only the remainder r but also cofactors $q_1, \ldots, q_m \in K[X_1, \ldots, X_n]$ such that $p - r = q_1 g_1 + \cdots + q_m g_m$ when applied to p and $G = \{g_1, \ldots, g_m\}$.

7⋆. Fill the gap in the proof of the implication 1 $\Rightarrow$ 2 of Theorem 4.77, i.e., show that if $G \subseteq K[X_1, \ldots, X_n]$ is such that every $u \in K[X_1, \ldots, X_n]$ has a unique remainder $\operatorname{red}(u, G)$, then we have $\operatorname{red}(u, G) = \operatorname{red}(u + c\tau \operatorname{lt}(g)^{-1} g, G)$ for every $c \in K$, every term τ, and every $g \in G$.

8. The set $G = \{D_x^3 - 5D_x^2 + 8D_x - 4, (4y + 1)D_x^2 - (16y + 4)D_x - yD_y + (15y + 4)\} \subseteq C(x, y)[D_x, D_y]$ is a Gröbner basis with respect to the lexicographic term order with $D_x < D_y$. Use Algorithm 4.73 to compute a Gröbner basis of $\langle G \rangle$ with respect to the lexicographic term order with $D_x > D_y$.

9⋆. Let $I \subseteq K[X_1, \ldots, X_n]$ be an ideal and G be a Gröbner basis of I. Show that the dimension of $K[X_1, \ldots, X_n]/I$ as a K-vector space is finite if and only if for every i there exists a $g \in G$ such that $\operatorname{lt}(g)$ is a power of X_i.

10. Let $I \subseteq K[X_1, \ldots, X_n]$ be an ideal and G be a Gröbner basis of I. Show that $1 \in I$ if and only if G contains an element of the form $uX_1^0 \cdots X_n^0$ with $u \in K \setminus \{0\}$.

11*. Let $I \subseteq K[X_1, \ldots, X_n]$, let $\leq_1, \leq_2$ be two term orders, and let G_1, G_2 be Gröbner bases of I with respect to $\leq_1, \leq_2$, respectively. Show that the number of terms τ with $\operatorname{red}_{\leq_1}(\tau, G_1) = \tau$ is equal to the number of terms τ with $\operatorname{red}_{\leq_2}(\tau, G_2) = \tau$. Must the sets of these terms also be equal?

12*. Show that $\{(1-k+n)S_n + (1+n), (1+k)S_k + 2(k-n)\} \subseteq C(n,k)[S_n, S_k]$ is a Gröbner basis and that $\{(1-k+n)S_n + (1+n), (1+k)S_k + 2(k+n)\}$ is not.

13. In line 2 of Algorithm 4.80, we do not initialize P with all pairs, as Theorem 4.79 suggests. Why is this okay?

14. A power series $a(x, y) \in C[[x, y]]$ has the annihilating ideal

$$\begin{aligned} I = \langle &(x-2)xD_xD_y + (2y+1)D_y^2 + (x+2)D_y, 4xD_x^2D_y - (x+4y+4)D_xD_y^2 \\ &+ (y+1)D_y^3 - 2xD_xD_y + (4y+7)D_y^2 - 4xD_x + 4(y+3)D_y\rangle \\ &\subseteq C(x,y)[D_x, D_y]. \end{aligned}$$

Show that the series is D-finite.

15. A sequence $(a_{n,k})_{n,k=0}^{\infty}$ has the annihilating ideal

$$\begin{aligned} I = \langle &(1+k)(k+n)S_k + (k-n)(1+k+n), \\ &(1-k+n)(k+n)S_n - (1+n)(1+k+n)\rangle \subseteq C[n,k][S_n, S_k]. \end{aligned}$$

Show that the sequence is holonomic.

16. In the commutative case, we have

$$\min(\operatorname{lexp}(p), \operatorname{lexp}(q)) = 0 \Rightarrow \operatorname{red}(\operatorname{spol}(p, q), \{p, q\}) = 0.$$

Show that this does not work in the noncommutative case.

17.** In the commutative case, we have the following criterion: whenever $B = \{b_1, \ldots, b_m\} \subseteq C[x_1, \ldots, x_n]$ and $p, u, v \in C[x_1, \ldots, x_n]$ are such that

1. there exist $q_1, \ldots, q_m \in C[x_1, \ldots, x_n]$ such that $\operatorname{spol}(u, p) = q_1b_1 + \cdots + q_mb_m$ and $\operatorname{lt}(q_ib_i) < X^{\max(\operatorname{lexp}(u), \operatorname{lexp}(p))}$ for all i,
2. there exist $q_1, \ldots, q_m \in C[x_1, \ldots, x_n]$ such that $\operatorname{spol}(p, v) = q_1b_1 + \cdots + q_mb_m$ and $\operatorname{lt}(q_ib_i) < X^{\max(\operatorname{lexp}(p), \operatorname{lexp}(v))}$ for all i, and
3. $\operatorname{lexp}(p) \leq \max(\operatorname{lexp}(u), \operatorname{lexp}(v))$,

then there also exist $q_1, \ldots, q_m \in C[x_1, \ldots, x_n]$ such that $\operatorname{spol}(u, v) = q_1b_1 + \cdots + q_mb_m$ and $\operatorname{lt}(q_ib_i) < X^{\max(\operatorname{lexp}(u), \operatorname{lexp}(v))}$ for all i.

Show that this also works in the noncommutative case.

18. Let $G \subseteq K[X_1, \ldots, X_n]$ be a Gröbner basis and $g, h \in G$ with $g \neq h$. Show that $\operatorname{lexp}(g) \leq \operatorname{lexp}(h)$ implies that also $G \setminus \{h\}$ is a Gröbner basis of $\langle G \rangle$.

19. In the ideal

$$\begin{aligned} I = \langle &(x-1)D_x S_n + (x-1)D_x - (1+n)S_n + (1+n), \\ &(x-1)^2(x+1)D_x^2 + (x-1)(n+2x+nx)D_x - n(1+n)S_n + n(1+n)\rangle \\ &\subseteq C(n,x)[S_n, D_x], \end{aligned}$$

find an element which is a $C(n,x)$-linear combination of powers of $S_n D_x$.

20. In the commutative case, an alternative way to compute the intersection of two ideals $I = \langle b_1, \ldots, b_m\rangle$ and $J = \langle d_1, \ldots, d_k\rangle$ of $C[x_1, \ldots, x_n]$ is to compute the elimination ideal

$$\langle tb_1, \ldots, tb_m, (1-t)d_1, \ldots, (1-t)d_k\rangle \cap C[x_1, \ldots, x_n],$$

where t is an additional variable. Does this also work in the noncommutative case?

References

Gröbner bases for ideals of a commutative polynomial ring $C[x_1, \ldots, x_n]$ were introduced by Buchberger in his Ph.D. thesis [117]. They play a central role in computer algebra. Introductory texts on the subject include [29, 47, 167].

A starting point for the development of Gröbner bases for non-commutative rings was the influential paper of Bergman from 1978 [56], who considered the case of a free algebra. In general, an ideal in such a ring need not have a finite Gröbner basis, so that during the 1980s, various people have investigated theories for Gröbner bases in more special non-commutative settings, including Galligo [200], Mora [332], Apel and Lassner [37], Takayama [422], Kandri-Rody and Weispfenning [256]. An introductory article of Mora [333] contains a proof of the non-commutative chain criterion (Exercise 17).

Zeilberger did not use Gröbner basis in his landmark paper [468], but suggested the use of Gröbner bases in this context. Chyzak and Salvy took up this suggestion and introduced Gröbner bases for Ore algebras [153, 154, 157].

The idea to view the reduction process from the perspective of linear algebra goes back to Lazard [305] and culminated in Faugère's F4 algorithm [189]. These techniques were developed for the commutative case but the extension to the non-commutative setting is straightforward. Less straightforward is the extension of another idea for speeding up Gröbner basis computation, which was introduced by Faugère under the name F5 [190] and has led to the development of so-called signature-based Gröbner bases algorithms [182]. A signature-based Gröbner bases algorithm for the non-commutative case was worked out by Sun, Wang, Ma, and Zhang [420].

Chapter 5
Summation and Integration

5.1 The Indefinite Problem

Informally, indefinite integration refers to the problem of finding an antiderivative for a given function, i.e., given f, the task is to find g such that $g' = f$. We may write such a g as $g = \int f$. If $'$ is the standard derivation, the problem is boring for polynomials, but it already becomes interesting for rational functions. One reason is that the integral of a rational function need not be a rational function. Whether or not a rational function integral g exists for a given f is easy to answer. We can simply solve the differential equation $g' = f$ for g, for example by using techniques from Sect. 3.5. This is sufficient for the decision problem ("does a rational integral exist?"), and it is perfectly satisfactory that the algorithm also supplies a g if there is one. But it is somewhat unsatisfactory that whenever the integral is not rational, the algorithm only informs us about this fact without providing any additional information. We can do better.

What prevents a rational function from having a rational integral are poles with multiplicity 1, because such poles cannot appear in the derivative of a rational function. For example, $f = 1/x$ cannot have a rational antiderivative $g = p/q$, because $g' = (p'q - pq')/q^2 = 1/x$ would force $x(p'q - pq') = q^2$, so $q \mid p'q - pq'$, so $q \mid pq'$. Since we may assume that $\gcd(p, q) = 1$, this further implies $q \mid q'$, which is impossible, because $\deg(q') < \deg(q)$.

It is possible to write a rational function as the sum of an integrable rational function and one that does not have any multiple poles. The idea is to successively subtract from f derivatives of rational functions that cancel the highest order poles in f. To see how this works, write $f = \frac{a}{uv^m}$ for some $a, u, v \in C[x]$ with $m \geq 2$ and $\deg a < \deg u + m \deg v$ and $\gcd(u, v) = \gcd(v, v') = \gcd(a, uv) = 1$. Note that the assumption $\gcd(v, v') = 1$ means that v is squarefree, i.e., v does not have multiple roots. We can think of u as containing all factors of the denominator whose multiplicities are less than m. We now want to find polynomials $b, c \in C[x]$ such that

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1_5

$$\frac{a}{uv^m} = \left(\frac{b}{v^{m-1}}\right)' + \frac{c}{uv^{m-1}} = \frac{b'v - b(m-1)v'}{v^m} + \frac{c}{uv^{m-1}}.$$

Multiply this equation by uv^m and take the equation modulo v to get the equation

$$a \equiv -(m-1)buv' \bmod v,$$

which has a unique solution $b \in C[x]$ with $\deg b < \deg v$ because of the assumptions $m \neq 1$ and $\gcd(v', v) = \gcd(u, v) = 1$. Knowing b, we can then determine $c = (a - b'uv + (m-1)buv')/v$. By the choice of b, the result will be a polynomial of degree less than $\deg u + (m-1)\deg v$. Repeated application of this procedure gives the following algorithm.

Algorithm 5.1 *(Hermite reduction)*
Input: $f \in C(x)$.
Output: $g, h \in C(x)$ *such that* $f = g' + h$ *and* h *has a squarefree denominator and its numerator degree is less than its denominator degree.*

1 *Write* $f = p + a/d$ *for* $p, a, d \in C[x]$ *with* $\deg a < \deg d$.
2 *Compute the squarefree decomposition* $d = d_1 d_2^2 \cdots d_m^m$ *of* d *(cf. part 1 of Theorem 1.25).*
3 *Set* $u = d_1 d_2^2 \cdots d_{m-1}^{m-1}$, $v = d_m$ *and* $g = \int p$.
4 *while* $m \geq 2$ *do*
5   *Find* b *and* c *as described above.*
6   *Set* $g = g + b/v^{m-1}$; $a = c$; $u = u/d_{m-1}^{m-1}$; $v = d_{m-1}$ *and then* $m = m - 1$.
7 *Return* g *and* $h = a/u$.

Theorem 5.2

1. *Algorithm 5.1 is correct. Applied to a rational function whose numerator and denominator have degree at most* n *and whose pole multiplicities are bounded by* m*, the algorithm requires no more than* $O(mM(n)\log(n))$ *operations in* C.
2. *A rational function* $f \in C(x)$ *is integrable in* $C(x)$ *if and only if* $h \in C(x)$ *as computed by Algorithm 5.1 is zero.* □

Proof

1. Correctness follows from the discussion above: the updates in line 6 are such that we have $f = g' + \frac{a}{uv^m}$ with $\deg a \leq \deg u + m \deg v$ in every iteration. For the complexity, the polynomial division in line 1 and the squarefree decomposition in line 2 cost $O(M(n)\log(n))$ operations. Furthermore, each execution of line 5 involves a call to the extended Euclidean algorithm (cf. Exercise 1) at the cost of $O(M(n)\log(n))$ operations, and the updates in line 6 are not more expensive than that. Altogether there are $m - 1$ iterations of the while loop, so the claim follows.

2. "⇐" is clear. "⇒": Observe that f is integrable in $C(x)$ if and only if $f - g'$ is integrable in $C(x)$ for every $g \in C(x)$. Therefore it suffices to show that a nonzero rational function h with squarefree denominator cannot be a derivative of a rational function. Assume otherwise, say $h = (p/q)'$ for some $p, q \in C[x]$. Let v be an irreducible factor of q and let $m \geq 1$ be its multiplicity, so that $q = uv^m$ for some u with $\gcd(p, u) = \gcd(v, u) = \gcd(v, v') = 1$. Then

$$\Big(\frac{p}{uv^m}\Big)' = \frac{p'uv - pu'v - mpuv'}{u^2v^{m+1}}.$$

Because of $\gcd(puv', v) = 1$ and $m \geq 1$, it follows that v does not divide the numerator, so v^{m+1} must divide the denominator of h, in contradiction to its squarefreeness. ■

Hermite reduction reduces the problem of integrating an arbitrary rational function f to the problem of integrating a rational function h with a squarefree denominator and a numerator whose degree is less than the degree of the denominator. A brutal way to integrate such a rational function is to consider its partial fraction decomposition

$$h = \sum_{k=1}^{n} \frac{c_k}{x - \alpha_k}$$

for $\alpha_1, \ldots, \alpha_n, c_1, \ldots, c_n \in \bar{C}$ and integrate it termwise. Note that a partial fraction $c/(x - \alpha)$ has the antiderivative $c \log(x - \alpha)$, so it follows that the indefinite integral of h can be written as a $\bar{C}$-linear combination of a finite number of logarithmic terms whose arguments are monic polynomials in x of degree 1. In particular, the integral of any rational function can be expressed as an elementary function.

In theory, this could be the end of the story, but in practice, computing the partial fraction decomposition of h is overkill, as it may lead us to compute with unnecessarily large algebraic extensions of the constant field.

Example 5.3

1. For $h = \frac{x}{x^2+1} \in \mathbb{Q}(x)$ we have

$$h = \frac{1/2}{x - \mathrm{i}} + \frac{1/2}{x + \mathrm{i}} = \Big(\frac{1}{2}\log(x - \mathrm{i}) + \frac{1}{2}\log(x + \mathrm{i})\Big)',$$

so the resulting integral lives in the differential field $\mathbb{Q}(\mathrm{i})(x, \log(x-\mathrm{i}), \log(x+\mathrm{i}))$, where the constant field contains i. But we also have the alternative representation

$$h = \frac{x}{x^2 + 1} = \Big(\frac{1}{2}\log(x^2 + 1)\Big)',$$

and here the integral lives in the differential field $\mathbb{Q}(x, \log(x^2+1))$. This representation not only avoids the extension of the constant field, but it also needs only one logarithm instead of two.

2. An extension of the constant field cannot always be avoided. For example, for $h = \frac{1}{x^2+1}$ we have

$$\frac{1}{x^2+1} = -\frac{\mathrm{i}/2}{x-\mathrm{i}} + \frac{\mathrm{i}/2}{x+\mathrm{i}} = \Big(-\frac{\mathrm{i}}{2}\log(x-\mathrm{i}) + \frac{\mathrm{i}}{2}\log(x+\mathrm{i})\Big)',$$

so the integral can be expressed as element of $\mathbb{Q}(\mathrm{i})(x, \log(x+\mathrm{i}), \log(x-\mathrm{i}))$. Unlike in the first example, the extension of the constant field is necessary, as we will see in the next theorem. □

Two terms $c_i \log(v_i)$, $c_j \log(v_j)$ in a linear combination $\sum_k c_k \log(v_k)$ can be merged like in the first example above whenever $c_i = c_j$. In this case, we can replace $\log(v_i) + \log(v_j)$ by $\log(v_i v_j)$. Our goal is therefore to identify partial fractions $c/(x-\alpha)$ in the partial fraction decomposition of h which share the same constant multiplier c, but without computing the partial fraction decomposition explicitly. Inspired by the terminology of complex analysis, we call $c \in \bar{C}$ the *residue* of $h \in C(x) \subseteq \bar{C}(x)$ at $\alpha \in C$ if the term $c/(x-\alpha)$ appears in the partial fraction decomposition of h and use the notation $\mathrm{Res}_{x-\alpha} h := c$. Be careful not to confuse this notation with the resultant $\mathrm{res}(p, q)$ of two polynomials $p, q \in C[x]$. When α is not a pole of h, we define $\mathrm{Res}_{x-\alpha} h := 0$. The key to efficient integration of h is that the relevant information about the residues of h can be obtained without explicitly computing its partial fraction decomposition.

Theorem 5.4 *Let $q \in C[x]$ be monic and squarefree, let $p \in C[x]$ with* $\deg p < \deg q$, *and let $h = \frac{p}{q}$.*

1. *For every root $\alpha \in \bar{C}$ of q, we have* $\mathrm{Res}_{x-\alpha} \frac{p}{q} = \frac{p(\alpha)}{q'(\alpha)}$.
2. *If $c \in \bar{C}$ and $\alpha_1, \ldots, \alpha_n \in \bar{C}$ are all of the roots of q with* $\mathrm{Res}_{x-\alpha} h = c$ *where $\alpha \in \{\alpha_1, \ldots \alpha_n\}$, then* $(x-\alpha_1)\cdots(x-\alpha_n) = \gcd(q, p - cq') \in C(c)[x]$.
3. *An element $c \in \bar{C}$ is a residue of h if and only if it is a nonzero root of the polynomial* $\mathrm{res}_x(q, p - zq') \in C[z]$.
4. *If $c_1, \ldots, c_n \in \bar{C}$ are the residues of h and* $v_k = \gcd(q, p - c_k q')$ *($k = 1, \ldots, n$), then $h = \sum_{k=1}^n c_k \frac{v_k'}{v_k}$, so an antiderivative of h is* $\sum_{k=1}^n c_k \log(v_k)$.
5. *If K is a subfield of $\bar{C}$, and $\tilde{c}_1, \ldots, \tilde{c}_m \in K$, $\tilde{v}_1, \ldots, \tilde{v}_m \in K(x)$ are such that $h = \sum_{k=1}^m \tilde{c}_k \frac{\tilde{v}_k'}{\tilde{v}_k}$, then K contains all residues of h.* □

Proof

1. Let $\alpha_1, \ldots, \alpha_n \in \bar{C}$ be all of the poles of h, say with $\alpha = \alpha_1$. Consider the partial fraction decomposition $h = \sum_{k=1}^n \frac{c_k}{x-\alpha_k}$ in $\bar{C}(x)$. Multiplying it by $x - \alpha_1$ and then setting x to α_1 gives

$$\frac{p(\alpha_1)}{\prod_{k=2}^{n}(\alpha_1 - \alpha_k)} = c_1,$$

so it remains to show that $q'(\alpha_1) = \prod_{k=2}^{n}(\alpha_1 - \alpha_k)$. Indeed, $q = (x - \alpha_1) \cdots (x - \alpha_n)$ implies $q' = \sum_{k=1}^{n} \prod_{i \neq k}(x - \alpha_i)$, and setting x to α_1 turns all products to zero except for the first.

2. By part 1 we have $x - \alpha_k \mid q$ and $x - \alpha_k \mid p - cq'$ for every k. Also, if $\alpha \in \bar{C}$ is a pole of h with some residue $\tilde{c} \neq c$, then $p/q' = \tilde{c} \bmod (x - \alpha)$ implies that $x - \alpha \nmid p - cq'$. Therefore, $x - \alpha$ is a common divisor of q and $p - cq'$ if and only if $\alpha \in \{\alpha_1, \ldots, \alpha_n\}$. Since the leading coefficients of $(x - \alpha_1) \cdots (x - \alpha_n)$ and $\gcd(q, p - cq')$ also agree, the two polynomials must be equal.
3. This follows directly from the previous part, since it is a general property of the resultant that $\gcd(u, v) \neq 1 \iff \operatorname{res}(u, v) = 0$.
4. We show that the difference $d = h - \sum_{k=1}^{n} c_k \frac{v_k'}{v_k}$ is zero. First observe that $q = \prod_{k=1}^{n} v_k$, because q and all of the v_k are monic and squarefree, and every root of q is also a root of precisely one of the v_k. Thus, expressing d with a common denominator gives $d = \frac{p - \sum_{k=1}^{n} c_k v_k' \prod_{i \neq k} v_i}{q}$. If α is any root of q, say a root of v_j for some j, then $\operatorname{Res}_{x-\alpha}(d) = \frac{p(\alpha) - c_j v_j'(\alpha) \prod_{i \neq j} v_i(\alpha)}{q'(\alpha)} = \frac{p(\alpha)}{q'(\alpha)} - c_j \frac{v_j'(\alpha) \prod_{i \neq j} v_i(\alpha)}{q'(\alpha)}$. Since $\frac{p(\alpha)}{q'(\alpha)} = \operatorname{Res}_{x-\alpha}(h) = c_j$, we are done if we can show that $v_j'(\alpha) \prod_{i \neq j} v_i(\alpha) = q'(\alpha)$. This is indeed the case, because $q = \prod_{k=1}^{n} v_k$ implies $q' = \sum_{k=1}^{n} v_k' \prod_{i \neq k} v_i$, and setting x to α turns all products to zero except the kth one.
5. Let $\tilde{w}_1, \ldots, \tilde{w}_\ell \in K[x]$ be squarefree, monic, and pairwise coprime so that for suitable integers $e_{i,j} \in \mathbb{Z}$ we can write $\tilde{v}_k = \prod_{j=1}^{\ell} \tilde{w}_j^{e_{k,j}}$ $(k = 1, \ldots, m)$. Such polynomials $\tilde{w}_j$ clearly exist: we can take for example all irreducible factors of $\tilde{v}_1, \ldots, \tilde{v}_m$. Since we have $\frac{(u^n v^m)'}{u^n v^m} = n\frac{u'}{u} + m\frac{v'}{v}$ for all $n, m \in \mathbb{Z}$ and all $u, v \in K[x]$ (Exercise 9 in Sect. 3.2), we have

$$h = \sum_{k=1}^{m} \tilde{c}_k \frac{\tilde{v}_k'}{\tilde{v}_k} = \sum_{k=1}^{m} \tilde{c}_k \sum_{j=1}^{\ell} e_{k,j} \frac{\tilde{w}_j'}{\tilde{w}_j} = \sum_{j=1}^{\ell} \left(\sum_{k=1}^{m} \tilde{c}_k e_{k,j} \right) \frac{\tilde{w}_j'}{\tilde{w}_j}.$$

For a pole $\alpha \in \bar{C}$ of h we therefore have

$$\operatorname{Res}_{x-\alpha} h = \sum_{j=1}^{\ell} \left(\sum_{k=1}^{m} \tilde{c}_k e_{k,j} \right) \operatorname{Res}_{x-\alpha} \frac{\tilde{w}_j'}{\tilde{w}_j}.$$

By part 1, we have $\operatorname{Res}_{x-\alpha} \frac{\tilde{w}_j'}{\tilde{w}_j} = 1$ when α is a root of $\tilde{w}_j$, and by the definition of residue, we have $\operatorname{Res}_{x-\alpha} \frac{\tilde{w}_j'}{\tilde{w}_j} = 0$ when α is not a root of $\tilde{w}_j$. Therefore, $\operatorname{Res}_{x-\alpha} h = \sum_{k=1}^{m} \tilde{c}_k e_{k,j}$ for some j. We have thus shown that $\operatorname{Res}_{x-\alpha} h \in K$. ■

The polynomial $\operatorname{res}_x(q, p - zq') \in C[z]$ appearing in part 3 of this theorem is called the Rothstein-Trager resultant. (Once more: be careful not to confuse residue and resultant in this context.) In order to integrate h, we first determine the nonzero roots $c_1, \dots, c_n$ of the Rothstein-Trager resultant. For each $k = 1, \dots, n$, we then compute $v_k = \gcd(q, p - c_k q') \in C(c_k)[x]$. The integral of h is then $\sum_{k=1}^n c_k \log(v_k)$.

Hermite reduction combined with the logarithmic part obtained via the Rothstein-Trager resultant allows us to express the integral of any given rational function as the sum of a rational function and a linear combination of logarithms. Other types of integrands require other techniques. Let us next consider the case when the given integrand f is hyperexponential and we want to decide whether $\int f$ can be expressed as a hyperexponential function as well, i.e., whether there exists a hyperexponential function g such that $g' = f$. In fact, we have already solved this problem in Sect. 3.6 as a special case of solving inhomogeneous linear differential equations with a hyperexponential right hand side (cf. Example 3.72). It is worthwhile to have a closer look at this special case.

Consider a hyperexponential function f over $C(x)$ specified through a given rational function $u \in C(x)$ such that $f'/f = u$. If there is a hyperexponential function g over $C(x)$ such that $g' = f$, then, since g' is a rational multiple of g, the terms f and g must be similar. Therefore, the search for such a g reduces to the search for a rational function w such that $g = wf$ meets the requirement $f = g'$. The requirement then translates into $f = w'f + wf' = w'f + wuf$, i.e., $w' + wu = 1$. Letting $q, r \in C[x]$ be the numerator and denominator of u, respectively, we arrive at the equation

$$rw' + qw = r,$$

in which $r, q \in C[x]$ are known and $w \in C(x)$ is unknown. Suppose that $p \in C[x]$ is an irreducible factor of multiplicity $i \in \mathbb{N} \setminus \{0\}$ of the denominator of a solution w, i.e., we can write $w = p^{-i}\tilde{w}$ for some rational function $\tilde{w}$ whose numerator and denominator is not a multiple of p. With $w' = -ip^{-i-1}p'\tilde{w} + p^{-i}\tilde{w}'$ the equation above turns into

$$rp\tilde{w}' + (qp - irp')\tilde{w} = rp^{i+1}.$$

Since p is contained as a factor in $rp\tilde{w}'$, $qp\tilde{w}$, and in rp^{i+1}, it must be contained as a factor in $irp'\tilde{w}$, and therefore in r, because $\gcd(p, p') = 1$ whenever p is irreducible. This is good news, because r is part of the input and we can use it to restrict the factors p that can possibly appear in the output.

Knowing that p divides r, it follows that p^2 divides rp and rp^{i+1}, so p^2 must also divide $qp - irp'$, so $p \mid q - irp'/p$. From $(r/p^i)' = irp'/p^{i+1} + r'/p^i$ we get $r' = p^i(r/p^i)' - irp'/p$, which together with $p \mid q - irp'/p$ implies $p \mid q - ir'$. Remembering that we have already noticed that $p \mid r$, it follows that we must in fact have $p \mid \gcd(r, q - ir')$. When q and r are coprime (as we may well assume), then there are only finitely many $i \in \mathbb{N}$ for which $\gcd(r, q - ir')$ is nontrivial.

We can identify them for example as the nonnegative integer roots of the resultant $\operatorname{res}_x(r, q - zr') \in C[z]$.

If the resultant does not have any nonnegative integer roots, we can be sure that any rational solution of the equation $w' + uw = 1$ is in fact a polynomial solution. Otherwise, we can achieve this situation by making an appropriate change of variables. Instead of writing $u = q/r$, let us write

$$u = \frac{q}{r} + \frac{p'}{p}$$

for some $p, q, r \in C[x]$ with $\gcd(r, q - ir') = 1$ for all $i \in \mathbb{N}$. (Here we no longer assume that p is irreducible.) This is called a *(differential) Gosper form* of u, and it is shown in Exercise 16 that every $u \in C(x)$ can be brought into such a form.

The equation $w' + wu = 1$ turns into $w' + w(q/r + p'/p) = 1$ and then into $pw' + w(pq/r + p') = p$. Setting $\tilde{w} = pw$, we get $\tilde{w}' = pw' + p'w$, which turns the equation into $\tilde{w}' + \tilde{w}q/r = p$. Now setting $\tilde{w} = yr$ so that $\tilde{w}' = y'r + yr'$ allows us to further simplify the equation to $(y'r + yr') + yq = p$, i.e., to

$$ry' + (q + r')y = p.$$

This is called the *(differential) Gosper equation* for the indefinite integration problem for f. By the reasoning discussed above, the requirement $\gcd(r, q - ir') = 1$ in the definition of the Gosper form implies that every rational solution $y \in C(x)$ of this equation is in fact a polynomial. We have thus derived the following integration algorithm.

Algorithm 5.5 *(Almkvist-Zeilberger)*
Input: *A hyperexponential function f, specified via a rational function $u \in C(x)$ such that $f'/f = u$.*
Output: *A hyperexponential function g such that $g' = f$, or $\perp$ if no such g exists.*

1 *Determine $p, q, r \in C[x]$ such that $u = \frac{q}{r} + \frac{p'}{p}$ and $\gcd(r, q - ir') = 1$ for all $i \in \mathbb{N}$, for example by the algorithm from Exercise 16.*
2 *Determine, if possible, a polynomial $y \in C[x]$ such that $ry' + (q + r')y = p$, for example by the algorithms from Sect. 3.5.*
3 *If no such y exists, return $\perp$, otherwise return $g = wf$ with $w = ry/p$.*

The Almkvist-Zeilberger algorithm solves the indefinite integration problem for hyperexponential functions: given a hyperexponential function f, we apply it to the rational function $u = f'/f$. If it returns a rational function w, then $\int f = wf$, and if it returns $\perp$, then $\int f$ is not hyperexponential.

Algorithm 5.5 was inspired by Gosper's algorithm for indefinite summation of hypergeometric terms, which appeared about 10 years earlier. There, we are given a hypergeometric term f and want to know whether there is a hypergeometric term g such that $\sigma(g) - g = f$. It is fair to consider such a g as an indefinite sum of f, because if $(f_n)_{n=0}^{\infty}$ is a sequence interpretation of the hypergeometric term f and

$(g_n)_{n=0}^{\infty}$ is a sequence interpretation of the hypergeometric term g, then the equation $\sigma(g) - g = f$ translates into $g_{k+1} - g_k = f_k$, and summing this equation over k gives $\sum_{k=0}^{n} f_k = g_{n+1} - g_0$, thanks to a telescoping effect.

In order to solve the telescoping equation $\sigma(g) - g = f$ for g, let $u \in C(x)$ be such that $\sigma(f)/f = u$ and observe that if a hypergeometric solution g exists, it will be similar to f, so we can make an ansatz $g = wf$ for an unknown rational function w. The equation $\sigma(g) - g = f$ then simplifies to $u\sigma(w) - w = 1$. We have seen in Exercise 7 of Sect. 2.6 that every rational function $u \in C(x)$ can be written as $u = \frac{\sigma(p)}{p}\frac{q}{\sigma(r)}$ for some polynomials $p, q, r \in C[x]$ with $\gcd(q, \sigma^i(r)) = 1$ for all positive integers i. This is called a *(discrete) Gosper form* of u.

Substituting a Gosper form for u into the equation $u\sigma(w) - w = 1$ and clearing denominators gives

$$\sigma(p)q\sigma(w) - p\sigma(r)w = p\sigma(r).$$

First setting $\tilde{w} = w/p$ turns this equation to $q\sigma(\tilde{w}) - \sigma(r)\tilde{w} = p\sigma(r)$, and next assuming that y is such that $\tilde{w} = ry$, the equation simplifies further to

$$q\sigma(y) - ry = p.$$

This is called the *(discrete) Gosper equation*. As for its differential analog, the main feature of this equation is that all of its rational solutions y must in fact be polynomials. Indeed, if a rational solution y of the equation has a nontrivial denominator and s is one of its irreducible factors, then there would be some $i_{\min}, i_{\max} \in \mathbb{Z}$ such that $\sigma^{i_{\min}}(s)$ and $\sigma^{i_{\max}}(s)$ are factors of the denominators but none of the polynomials $\sigma^i(s)$ with $i < i_{\min}$ or $i > i_{\max}$ would appear in the denominator. This is simply because the denominator can have only finitely many factors. Now observe that the denominator of $\sigma(y)$ has the factor $\sigma^{i_{\max}+1}(s)$, which is not in the denominator of ry or of p, so it must be canceled by q. Likewise, the denominator of y has the factor $\sigma^{i_{\min}}(s)$, which is not in the denominator of $q\sigma(y)$ or p, so it must be canceled by r. But then $\sigma^{i_{\min}}(s) \mid r$ and $\sigma^{i_{\max}+1}(s) \mid q$ implies that $\sigma^{i_{\max}+1}(s) \mid \gcd(q, \sigma^{i_{\max}-i_{\min}+1}(r))$, and this is exactly what the condition in the definition of the Gosper form excludes.

In summary, Gosper's algorithm proceeds almost exactly as the Almkvist-Zeilberger algorithm:

Algorithm 5.6 *(Gosper)*
Input: *A hypergeometric term f, specified by a rational function $u \in C(x)$ such that $\sigma(f)/f = u$.*
Output: *A hypergeometric term g such that $\sigma(g) - g = f$, or $\perp$ if no such g exists*

1. *Determine $p, q, r \in C[x]$ such that $u = \frac{\sigma(p)}{p}\frac{q}{\sigma(r)}$ and $\gcd(q, \sigma^i(r)) = 1$ for all $i \in \mathbb{N}$, for example by the algorithm from Exercises 6 and 7 in Sect. 2.6.*
2. *Determine, if possible, a polynomial $y \in C[x]$ such that $q\sigma(y) - ry = p$, for example by the algorithms from Sect. 2.5.*

3 *If no such y exists, return $\perp$, otherwise return $g = wf$ with $w = ry/p$.*

Some people say that Gosper's algorithm "succeeds" if it returns a hypergeometric term g as specified and that it "fails" otherwise. Such statements should be avoided, because it is not the fault of the algorithm if it does not find a solution when no solution exists. Instead, it is better to say that f is "summable" or "Gosper-summable" if Gosper's algorithm returns a term g and that it is "not summable" (or "not Gosper-summable") if it returns $\perp$.

Example 5.7

1. In order to simplify the sum $\sum_{k=1}^{n} \frac{k}{k+1} 4^{-k}\binom{2k}{k}$, we consider the hypergeometric term f with $\sigma(f)/f = \frac{(2x+1)(x+1)}{2x(x+2)} =: u$, because

$$\frac{\frac{k+1}{k+2} 4^{-(k+1)}\binom{2(k+1)}{k+1}}{\frac{k}{k+1} 4^{-k}\binom{2k}{k}} = \frac{(2k+1)(k+1)}{2k(k+2)}.$$

A Gosper form of u is given by $p = x$, $q = 2x+1$, and $r = 2(x+1)$, so the Gosper equation for this summation problem reads

$$(2x+1)\sigma(y) - 2(x+1)y = x.$$

It has the solution $y = x+1$, so we can take $g = \frac{yq}{p} f = \frac{2(x+1)^2}{x} f$ as a solution of the telescoping equation $\sigma(g) - g = f$. Translated into traditional expressions, this gives the closed form

$$\begin{aligned}
&\sum_{k=1}^{n} \frac{k}{k+1} 4^{-k}\binom{2k}{k} \\
&= 2\frac{(n+2)^2}{n+1}\frac{n+1}{n+2} 4^{-(n+1)}\binom{2(n+1)}{n+1} - 2\frac{(1+1)^2}{1}\frac{1}{1+1} 4^{-1}\binom{2(1)}{1} \\
&= 2(n+2)4^{-(n+1)}\binom{2(n+1)}{n+1} - 2.
\end{aligned}$$

Such translations from algebraic objects to summation identities about sequences must be done carefully, because the multiplier w found by the algorithm may have singularities in the summation range. It then has to be checked manually to what extent the summation identity holds.

2. Gosper's algorithm can prove that the harmonic numbers $\sum_{k=1}^{n} \frac{1}{k}$ do not form a hypergeometric sequence. We apply it to $u = (\frac{1}{x+1})/(\frac{1}{x}) = x/(x+1)$. A Gosper form for this rational function is given by $p = 1$ and $q = r = x$, so the Gosper equation for this summation problem reads $x\sigma(y) - xy = 1$, and it is easily seen by inspection that this equation cannot have a polynomial solution y. □

The close analogy between the algorithms of Gosper and Almkvist-Zeilberger suggests once more that it might be better to approach the problem of summation and integration from the perspective of Ore algebras. Translated to this setting, we have in both cases an Ore algebra $K[\partial]$ acting on a $K[\partial]$-module M with $\dim_K(M) = 1$, and for a given element $f \in M$, the question is whether a certain first order inhomogeneous equation $(\partial - \beta) \cdot g = f$ admits a solution g in M. In the case of integration, ∂ is a derivation and we take $\beta = 0$. In the case of summation, taking the shift as ∂, we choose $\beta = 1$ so that $\partial - \beta$ is the forward difference.

For sums/integrals whose summand/integrand is D-finite but not necessarily hypergeometric/hyperexponential, we need to work with $K[\partial]$-modules M whose dimension over K may be greater than 1. Still, D-finiteness allows us to assume that $\dim_K(M)$ is finite, say M is generated by $e_1, \ldots, e_r$ as a K-vector space. Any summand/integrand in M can then be written as $P = p_1e_1 + \cdots + p_re_r$ for certain $p_1, \ldots, p_r \in K$, and the summation/integration problem consists of deciding whether there is an element $Q = q_1e_1 + \cdots + q_re_r \in M$ such that $(\partial - \beta) \cdot Q = P$. Making an ansatz for such a Q and expanding the left hand side, we get the condition

$$\sum_{k=1}^{r} \big(\sigma(q_k)(\partial \cdot e_k) + (\delta(q_k) - \beta q_k)e_k\big) = \sum_{k=1}^{r} p_k e_k.$$

In order to expand this further, let $A = ((a_{i,j}))_{i,j=1}^{r} \in K^{r\times r}$ be such that $\partial \cdot e_j = \sum_{i=1}^{r} a_{i,j}e_i$ for $j = 1, \ldots, r$. Coefficient comparison then leads to

$$A \begin{pmatrix} \sigma(q_1) \\ \vdots \\ \sigma(q_r) \end{pmatrix} + \begin{pmatrix} \delta(q_1) \\ \vdots \\ \delta(q_r) \end{pmatrix} - \beta \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_r \end{pmatrix}.$$

If we assume, as we may, that $K[\partial]$ is such that $\sigma = \mathrm{id}$ or $\delta = 0$, then this is a first order inhomogeneous coupled system of functional equations which can be solved with the techniques discussed in Sect. 4.3. We can thus formulate the following generic summation/integration algorithm for D-finite functions:

Algorithm 5.8
Input: *An element* $P = p_1e_1 + \cdots + p_re_r$ *of a* $K[\partial]$*-module* M *generated by* $e_1, \ldots, e_r$, *where* $K[\partial]$ *is an Ore algebra with* $\sigma = \mathrm{id}$ *or* $\delta = 0$, *and a constant* β.
Output: *An element* $Q = q_1e_1 + \cdots + q_re_r$ *of* M *such that* $(\partial - \beta) \cdot Q = P$, *or* $\perp$ *if no such* Q *exists.*

1 *Construct the matrix* $A = ((a_{i,j}))_{i,j=1}^{r} \in K^{r\times r}$ *with* $\partial \cdot e_j = \sum_{i=1}^{r} a_{i,j}e_i$ *for* $j = 1, \ldots, r$.
2 *If* $\sigma = \mathrm{id}$, *then solve the coupled linear system*

$$A\begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} + \begin{pmatrix} \delta(q_1) \\ \vdots \\ \delta(q_r) \end{pmatrix} - \beta \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_r \end{pmatrix}$$

for $q_1, \ldots, q_r$.

3 *Otherwise, solve the coupled linear system*

$$A\begin{pmatrix} \sigma(q_1) \\ \vdots \\ \sigma(q_r) \end{pmatrix} - \beta \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_r \end{pmatrix}$$

for $q_1, \ldots, q_r$.

4 *If there is a solution, return* $q_1 e_1 + \cdots + q_r e_r$ *as the answer. Otherwise return* $\perp$.

Example 5.9

1. Suppose we want to simplify the integral $\int x^3 J_1(x)^2 dx$, where $J_1(x)$ is the first Bessel function of the first kind. If $J_0(x)$ is the zeroth Bessel function of the first kind, we have the relations

$$J_0'(x) = -J_1(x) \quad \text{and} \quad J_1'(x) = J_0(x) - x^{-1} J_1(x),$$

which can be used to construct a suitable $\mathbb{Q}(x)[D]$-module. If we take $M = \mathbb{Q}(x)^3$ and specify

$$\begin{aligned} D \cdot e_1 &= -2e_2, \\ D \cdot e_2 &= e_1 - x^{-1} e_2 - e_3, \\ D \cdot e_3 &= 2e_2 - 2x^{-1} e_3, \end{aligned}$$

then the unit vectors $e_1, e_2, e_3 \in M$ correspond to the expressions $J_0(x)^2$, $J_0(x)J_1(x)$, and $J_1(x)^2$, respectively. The integrand expression corresponds to the vector $P = (0, 0, x^3) \in M$, and a vector $Q = (q_1, q_2, q_3) \in M$ satisfies $D \cdot Q = P$ if and only if its coordinates q_1, q_2, q_3 satisfy the system

$$\begin{pmatrix} 0 & 1 & 0 \\ -2 & -1/x & 2 \\ 0 & -1 & -2/x \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} + \begin{pmatrix} q_1' \\ q_2' \\ q_3' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x^3 \end{pmatrix}.$$

The unique solution of this system is $(q_1, q_2, q_3) = (\frac{1}{6}x^4, -\frac{2}{3}x^3, \frac{1}{6}(4x^2 + x^4))$, which implies that

$$D \cdot \left(\tfrac{1}{6}x^4 J_0(x)^2 - \tfrac{2}{3}x^3 J_0(x)J_1(x) + \tfrac{1}{6}(4x^2 + x^4)J_1(x)^2\right) = x^3 J_0(x)^2,$$

so we have $\int x^3 J_0(x)^2 dx = \frac{1}{6}x^4 J_0(x)^2 - \frac{2}{3}x^3 J_0(x)J_1(x) + \frac{1}{6}(4x^2 + x^4)J_1(x)^2$.

2. Suppose we want to simplify the sum $\sum_{k=0}^{n}(2k+1)P_k(x)P_k(y)$, where P_k denotes the kth Legendre polynomial. The Legendre polynomials satisfy the recurrence

$$(n+2)P_{n+2}(z) - (2n+3)zP_{n+1}(z) + (n+1)P_n(z) = 0 \qquad (n \geq 0).$$

We choose $M = \mathbb{Q}(x, y, n)^4$ and turn M into a $\mathbb{Q}(x, y, n)[S]$-module by specifying

$$\begin{aligned}
S \cdot e_1 &= e_4,\\
S \cdot e_2 &= -\tfrac{n+1}{n+2}e_3 + \tfrac{(2n+3)x}{n+2}e_4,\\
S \cdot e_3 &= -\tfrac{n+1}{n+2}e_2 + \tfrac{(2n+3)y}{n+2}e_4,\\
S \cdot e_4 &= \tfrac{(n+1)^2}{(n+2)^2}e_1 - \tfrac{(n+1)(2n+3)x}{(n+2)^2}e_2 - \tfrac{(n+1)(2n+3)y}{(n+2)^2}e_3 + \tfrac{(2n+3)^2xy}{(n+2)^2}e_4,
\end{aligned}$$

so that the unit vectors $e_1, e_2, e_3, e_4 \in M$ correspond to the expressions

$$P_n(x)P_n(y),\ P_{n+1}(x)P_n(y),\ P_n(x)P_{n+1}(y),\ P_{n+1}(x)P_{n+1}(y),$$

respectively. The summand expression corresponds to the vector $P = (2n+1, 0, 0, 0) \in M$, and a vector $Q = (q_1, q_2, q_3, q_4) \in M$ satisfies $(S-1)\cdot Q = P$ if and only if its coordinates $q_1, \ldots, q_4$ satisfy the system

$$\begin{pmatrix} 0 & 0 & 0 & \frac{(n+1)^2}{(n+2)^2} \\ 0 & 0 & -\frac{n+1}{n+2} & -\frac{(n+1)(2n+3)x}{(n+2)^2} \\ 0 & -\frac{n+1}{n+2} & 0 & -\frac{(n+1)(2n+3)y}{(n+2)^2} \\ 1 & \frac{(2n+3)x}{n+2} & \frac{(2n+3)y}{n+2} & \frac{(2n+3)^2xy}{(n+2)^2} \end{pmatrix} \begin{pmatrix} \sigma(q_1) \\ \sigma(q_2) \\ \sigma(q_3) \\ \sigma(q_4) \end{pmatrix} - \begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix} = \begin{pmatrix} 2n+1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The unique solution of this system is $Q = (-2n-1, \frac{n+1}{x-y}, -\frac{n+1}{x-y}, 0)$, which implies that for

$$g_k := -(2k+1)P_k(x)P_k(y) + \tfrac{k+1}{x-y}P_{k+1}(x)P_k(y) - \tfrac{k+1}{x-y}P_k(x)P_{k+1}(y)$$

we have $g_{k+1} - g_k = (2k+1)P_k(x)P_k(y)$ $(k \geq 0)$. Summing this equation for k from 0 to n gives

$$\sum_{k=0}^{n}(2k+1)P_k(x)P_k(y) = g_{n+1} - g_0,$$

which can be cleaned up to $g_{n+1} - g_0 = \frac{n+1}{x-y} P_{n+1}(x)P_n(y) - \frac{n+1}{x-y} P_n(x)P_{n+1}(y)$ using the initial values P_0, P_1 and the recurrence for rewriting P_{n+2} in terms of P_n and P_{n+1}. □

If M is a $K[\partial]$-module for which we do not have a basis at hand, we can still ask whether a given D-finite element $f \in M$ admits a sum/integral $g \in M$ which can be written as $g = Q \cdot f$ for some $Q \in K[\partial]$. If $L \in K[\partial]$ is a minimal order annihilating operator of f, then $g = Q \cdot f$ combined with $(\partial - \beta) \cdot g = f$ gives $((\partial - \beta)Q - 1) \cdot f = 0$, i.e., $\operatorname{rrem}((\partial - \beta)Q - 1, L) = 0$. Viewed from this perspective, it is not necessary to assume that $\sigma = \mathrm{id}$ or $\delta = 0$. It is better to assume instead that ∂ acts as a σ-derivation, so that we have $\beta = 0$ in both the integration and the summation case. Let us use the symbol Δ instead of ∂ in order to emphasize this assumption. If $r = \operatorname{ord}(L)$, it suffices to search for an operator Q with $\operatorname{ord}(Q) < r$, because $Q \cdot f = \operatorname{rrem}(Q, L) \cdot f$. Given an operator L of order r, the question is thus whether there exists an operator Q of order at most $r - 1$ such that $\operatorname{rrem}(\Delta Q - 1, L) = 0$.

We will see that adjoints can help us to answer this question. Recall that in Sect. 4.4 we introduced the adjoint algebra $K[\Delta^*]$ of $K[\Delta]$ as the Ore algebra with $\sigma^* = \sigma^{-1}$ and $\delta^* = -\delta \circ \sigma^{-1}$ in the role of σ and δ. The adjoint of an operator $L = \ell_0 + \ell_1\Delta + \cdots + \ell_r\Delta^r \in K[\Delta]$ is defined as $L^* := \ell_0 + \Delta^*\ell_1 + \cdots + (\Delta^*)^r\ell_r \in K[\Delta^*]$. To see how adjoints enter the game, note that the product rule $\delta(uv) = \delta(u)\sigma(v) + u\delta(v)$ $(u, v \in K)$ implies

$$\begin{aligned}
\delta\big(\delta^2(u)\sigma^{-1}(v)\big) &= \delta^3(u)v + \delta^2(u)(\delta\circ\sigma^{-1})(v)\\
\delta\big(\delta(u)\sigma^{-1}((\delta\circ\sigma^{-1})(v))\big) &= \delta^2(u)(\delta\circ\sigma^{-1})(v) + \delta(u)(\delta\circ\sigma^{-1})^2(v)\\
\delta\big(u\sigma^{-1}((\delta\circ\sigma^{-1})^2(v))\big) &= \delta(u)(\delta\circ\sigma^{-1})^2(v) + u(\delta\circ\sigma^{-1})^3(v).
\end{aligned}$$

Adding the first and the third equation and subtracting the second produces some pretty cancellations and leaves us with

$$\delta^3(u)v+u(\delta^*)^3(v)=\delta\big(\delta^2(u)\sigma^{-1}(v)-\delta(u)\sigma^{-1}((\delta\circ\sigma^{-1})(v))+u\sigma^{-1}((\delta\circ\sigma^{-1})^2(v))\big).$$

More generally, for every $i \in \mathbb{N}$ and every $u, v \in K$ we have

$$\delta^i(u)v - (-1)^i u(\delta^*)^i(v) = \delta\Bigg(\sum_{j=0}^{i-1}(-1)^j\delta^j(u)\sigma^{-1}((\delta^*)^{i-1-j}(v))\Bigg).$$

Replacing v by $\ell_i v$ and summing this equation for $i = 0, \ldots, r$ gives

$$v(L \cdot u) - u(L^* \cdot v) = \delta\Bigg(\underbrace{\sum_{i=0}^{r}\sum_{j=0}^{i-1}(-1)^j\delta^j(u)\sigma^{-1}((\delta^*)^{i-1-j}(\ell_i v))}_{=:\pi(u,v)}\Bigg).$$

This equation is called *Lagrange's identity*, and the bilinear function $\pi : K \times K \to K$ defined by the argument of δ on the right hand side is called the *concomitant* of L. Note that for every fixed choice of $v \in K$ there is an operator $Q \in K[\Delta]$ of order at most $r-1$ such that $Q \cdot u = \pi(u, v)$ for all $u \in K$. Therefore, if $v \in K$ is such that $L^* \cdot v = -1$, then Lagrange's identity provides us with an operator Q having the desired property $vL = \Delta Q - 1$, i.e., $\operatorname{rrem}(\Delta Q - 1, L) = 0$. According to the following proposition, the converse is also true.

Instead of expressing an indefinite sum/integral g in terms of f, we can also ask for an annihilating operator of such a g. An easy answer to this question is the operator $L\Delta$, because $\Delta \cdot g = f$ implies $(L\Delta) \cdot g = L \cdot (\Delta \cdot g) = L \cdot f = 0$. A more interesting question is whether there is also an annihilating operator of lower order. According to the following proposition, this too is equivalent to the existence of a $v \in K$ with $L^* \cdot v = -1$.

Proposition 5.10 *Let $K[\Delta]$ be an Ore algebra whose natural action on K is such that $\Delta \cdot 1 = 0$. Let M be a $K[\Delta]$-module and $f \in M$ be a D-finite element. Let $L \in K[\Delta] \setminus \{0\}$ be an annihilating operator of f of minimal order. Then the following statements are equivalent:*

1. *There is a $v \in K$ such that $L^* \cdot v = 1$.*
2. *There is a $Q \in K[\Delta]$ such that for $g := Q \cdot f$ we have $\Delta \cdot g = f$.*
3. *There is an element $g \in M$ with $\Delta \cdot g = f$ whose minimal annihilating operator has the same order as L.* □

Proof $1 \Rightarrow 2$. We show that there is a $Q \in K[\Delta]$ such that $(\Delta Q - 1) \cdot f = 0$. Let $v \in K$ be such that $L^* \cdot v = -1$, and let $Q \in K[\Delta]$ and $u \in K$ be such that $vL = \Delta Q + u$. Taking adjoints gives $L^* v = Q^* \Delta^* + u$, because $v^* = v$ and $u^* = u$. By $\Delta \cdot 1 = 0$, we have $\Delta^* \cdot 1 = 0$, so we find $-1 = L^* \cdot v = (L^* v) \cdot 1 = (Q^* \Delta^* + u) \cdot 1 = 0 + u$, as required.

$2 \Rightarrow 1$. We may assume that $\operatorname{ord}(Q) \le r - 1$, because $Q \cdot f = \operatorname{rrem}(Q, L) \cdot f$, so we can replace Q with $\operatorname{rrem}(Q, L)$ if needed. Then $\operatorname{ord}(\Delta Q) \le r$, so from $\operatorname{rrem}(\Delta Q - 1, L) = 0$ it follows that there is a $v \in K$ such that $\Delta Q - 1 = vL$. Taking adjoints gives $Q^* \Delta^* - 1 = L^* v$, and applying both sides to 1 gives $-1 = L^* \cdot v$, as claimed.

$2 \Rightarrow 3$. Assume again that $\operatorname{ord}(Q) \le r - 1$. For the operator $W = 1 - Q\Delta$ we then have $\operatorname{ord}(W) \le r$ and $(1 - Q\Delta) \cdot g = g - Q \cdot f = 0$.

$3 \Rightarrow 2$. If W is an annihilating operator of g of order $r = \operatorname{ord}(L)$, then W cannot contain Δ as a right factor, because if we had $W = U\Delta$ for some $U \in K[\Delta]$, then $W \cdot g = 0$ and $\Delta \cdot g = f$ would imply $U \cdot f = 0$, in contradiction to $\operatorname{ord}(U) = r - 1$ and L being a minimal order annihilating operator of f. We therefore have $W = Q\Delta - v$ for some $v \in K \setminus \{0\}$ and some $Q \in K[\Delta]$. Applying both sides to g, we obtain $0 = W \cdot g = (Q\Delta) \cdot g - vg = Q \cdot f - vg$, so we have $g = v^{-1} Q \cdot f$, which is a representation of the required form. ■

Example 5.11

1. Consider again the integral $\int x^3 J_1(x)^2 dx$. The integrand $f(x) = x^3 J_1(x)^2$ is annihilated by

$$L = x^3 D^3 - 6x^2 D^2 + x(15 + 4x^2)D - (15 + 8x^2),$$

but not by any operator of lower order. Using $D^* = -D$, we find

$$L^* = -x^3 D^3 - 15x^3 D^2 - x(57 - 4x^2)D - (20x^2 + 48).$$

The inhomogeneous differential equation $L^* \cdot v = -1$ has the solution $v = 1/(12x^2)$, so according to the proposition, the integral can be expressed in terms of the integrand and its derivatives. Indeed, for

$$Q = \frac{x}{12} D^2 - \frac{7}{12} D + \frac{4x^2 + 15}{12x}$$

we have $DQ - 1 = vL$, so

$$\int f(x)dx = \frac{4x^2 + 15}{12x} f(x) - \frac{7}{12} f'(x) + \frac{x}{12} f''(x).$$

Moreover, the integral is annihilated by the 3rd order operator

$$-\frac{x}{12} D^3 + \frac{7}{12} D^2 - \frac{4x^2 + 15}{12x} D + 1.$$

2. Now consider the integral $\int x^4 J_1(x)^2 dx$. An annihilating operator of minimal order for the integrand $f(x) = x^4 J_1(x)^2$ is

$$L = x^3 D^3 - 9x^2 D^2 + x(33 + 4x^2)D - 12(x^2 + 4).$$

Its adjoint is

$$L^* = -x^3 D^3 - 18x^2 D^2 - x(4x^2 + 87) - 3(8x^2 + 35).$$

Since the inhomogeneous equation $L^* \cdot v = -1$ has no solution in $C(x)$, it follows that the integral cannot be expressed in terms of f and its derivatives. Moreover, a minimal-order annihilating operator of the integral is

$$LD = x^3 D^4 - 9x^2 D^3 + x(33 + 4x^2)D^2 - 12(x^2 + 4)D.$$

□

Exercises

1. In the derivation of Hermite reduction, it was claimed that the equation $a \equiv -(m-1)buv' \bmod v$ has a unique solution $b \in C[x]$ with $\deg(b) < \deg(v)$ if $m > 1$ and $a, u, v \in C[x]$ are such that $\gcd(u, v) = \gcd(v', v) = 1$. Check this. How can this solution be found?

2*. Here is an alternative to Hermite's algorithm, due to Ostrogradsky. Let $f = \frac{a}{d} \in C(x)$ with $\deg a < \deg d$, and let $d = d_1 d_2^2 \cdots d_m^m$ be the squarefree decomposition of d. In order to find $f = g' + h$, we make an ansatz for

$$g = \frac{g_0 + g_1 x + \cdots + g_n x^n}{d_2 d_3^2 \cdots d_m^{m-1}} \quad \text{and} \quad h = \frac{h_0 + h_1 x + \cdots + h_k x^k}{d_1 d_2 \cdots d_m}$$

with undetermined constants $g_0, \ldots, g_n, h_0, \ldots, h_k$. Expressing $g' + h - f$ with a common denominator and equating the coefficients of the numerator to zero gives a linear system over C for the undetermined constants, which we solve for.

a. Determine choices for n and k for which the linear system has a solution.
b. Is the solution unique?
c. Estimate the cost of this algorithm.

3*. Show that every rational function admits a unique partial fraction decomposition. More precisely:

a. For every rational function $\frac{u}{pq}$ with $\deg(u) < \deg(pq)$ and $\gcd(p, q) = 1$ there exist unique $s, t \in C[x]$ such that $\deg s < \deg p$ and $\deg t < \deg q$ and $\frac{u}{pq} = \frac{s}{p} + \frac{t}{q}$.
b. For every rational function $\frac{u}{p^n}$ with $\deg(u) < n \deg(p)$ there exist unique $s \in C[x]$ and $t \in C[x]$ such that $\deg(s) < \deg(p)$ and $\deg(t) < (n-1)\deg(p)$ and $\frac{u}{p^n} = \frac{s}{p^n} + \frac{t}{p^{n-1}}$.

4. Prove or disprove:

a. For all $p, q \in C[x]$ and all $\alpha \in \bar{C}$ we have $\operatorname{Res}_{x-\alpha} \frac{p}{q} = \frac{p(\alpha)}{q'(\alpha)}$.
b. $r \in C(x)$ is a polynomial if and only if $\operatorname{Res}_{x-\alpha} r = 0$ for all $\alpha \in \bar{C}$.
c. For any $\alpha \in C$, the map $\operatorname{Res}_{x-\alpha} \colon C(x) \to C$ is C-linear.

5*. Let $p, q \in C[x]$ be such that q is squarefree, $0 \le \deg(p) < \deg(q)$, and $\gcd(p, q) = 1$. Can it happen that the Rothstein-Trager resultant for p and q **a.** has zero as a root? **b.** has multiple roots? **c.** has no roots at all? **d.** is the zero polynomial?

6. Simplify the following integrals:

a. $\int \frac{3x^4 - 5x^3 + 2x^2 - 18x - 12}{2x^3(x+1)^2} dx$; **b.** $\int \frac{4(x+1)(2x-1)}{(2x^2-1)^2} dx$;
c. $\int \frac{7x^4 + 2x^3 + 2x^2 - 9x + 20}{x^5} dx$; **d.** $\int \frac{1}{(x-2)^3(x-1)^2 x} dx$.

7. It is clear that the indefinite integral of a polynomial is always a polynomial. Show that also the indefinite sum of a polynomial is always a polynomial, i.e., for all $f \in C[x]$ there exists a $g \in C[x]$ such that $g(x+1) - g(x) = f(x)$.

8*.** (Peter Paule) This exercise is about a summation analog of Hermite reduction. For $p \in C[x]$ and $m \in \mathbb{N}$, we use the notation $\sigma^{\overline{m}}(p) = p\sigma(p)\cdots\sigma^{m-1}(p)$. By $\sigma\colon C(x) \to C(x)$ we mean the automorphism that maps x to $x+1$. Let $f = \frac{a}{d} \in C(x)$ with $\deg a < \deg d$.

a. Show that if there exists $g \in C(x)$ with $\Delta g = f$, then there exist $v \in C[x]$ with $\deg v \geq 1$ and $m \in \mathbb{N}$ with $m \geq 1$ such that $v \mid d$ and $\sigma^m(v) \mid d$.

b. Let $m \in \mathbb{N}$ be maximal such that there is a $v \in C[x]$ with $\deg v \geq 1$ and $v \mid d$ and $\sigma^{m-1}(v) \mid d$. Suppose that $m > 1$. Show that $\gcd(v, \sigma^{m-1}(v)) = 1$.

c. Let $m \in \mathbb{N}$ be as in part b. Show that f can be written as $\frac{\tilde{a}}{u\sigma^{\overline{m}}(v)}$ for some $\tilde{a}, u, v \in C[x]$ with $\deg \tilde{a} < \deg u + m \deg v$ and $\gcd(u, v) = 1$.

d. Let $m, \tilde{a}, u, v$ be as in part c. Suppose that $m > 1$. Show that there are $b, c \in C[x]$ such that

$$\frac{\tilde{a}}{u\sigma^{\overline{m}}(v)} = \Delta \frac{b}{\sigma^{\overline{m-1}}(v)} + \frac{c}{u\sigma^{\overline{m-1}}(\sigma(v))}.$$

e. Simplify the indefinite sum $\sum_{k=1}^{n} \frac{1}{(k+1)(k+3)}$.

9. Simplify the following integrals:

a. $\int (3x^4 + 14x^3 + 1) \exp(x^3 + x^2 + x) dx$;

b. $\int \frac{x^3 - 7x + 3}{(1-x)^3} \exp\left(\frac{x^2}{x-1}\right) dx$;

c. $\int x^{-\sqrt{2}}(x+1)^{\sqrt{2}}(x^2 + 3x - \sqrt{2} + 1) \exp(x) dx$;

d. $\int \frac{16x^3 - 7}{\sqrt{x^2 + x + 1}} dx$.

10. Show that the error function $\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z \exp(-t^2) dt$ is not hyperexponential.

11. Suppose that $f(x)$ is a hyperexponential function for which $\int f(x) dx$ is not hyperexponential. Under which circumstances can there still be a closed form of the form

$$\int f(x) dx = g(x) + \gamma_1 \log(h_1(x)) + \cdots + \gamma_k \log(h_k(x))$$

where $\gamma_1, \ldots, \gamma_k$ are constants and $g(x), h_1(x), \ldots, h_k(x)$ are hyperexponential functions?

12. Prove or disprove: A hyperexponential function can be integrated arbitrarily often if and only if it is of the form $p(x) \exp(\alpha x)$ where α is a constant and p is a polynomial.

13. Determine all $\alpha \in C$ for which $\int x\sqrt{x + \alpha} \exp(x) dx$ is hyperexponential.

14. Let h be hyperexponential over $C(x)$ and consider the differential ring $R = C(x)[h]$. Assume that h is transcendental over $C(x)$ and that $\operatorname{Const}(R) = C$. Design an algorithm which for any given $f \in R$ decides whether there is a $g \in R$ such that $g' = f$.

Hint: Exploit that h^i and h^j are not similar when $i \neq j$.

15⋆. Design an algorithm which for any given $f \in C(x)[\log(x)]$ decides whether there is a $g \in C(x)[\log(x)]$ such that $g' = f$.

16⋆. Show that for every $\frac{u}{v} \in C(x)$ there exist $p, q, r \in C[x]$ such that $\frac{u}{v} = \frac{q}{r} + \frac{p'}{p}$ and $\gcd(r, q - ir') = 1$ for all $i \in \mathbb{N}$.

17.

a. Let f be a hyperexponential function and $p, q, r \in C[x]$ be such that $\frac{q}{r} + \frac{p'}{p}$ is a Gosper form for f. Let $u \in C[x]$ and $g = uf$. Show that $\frac{q}{r} + \frac{(up)'}{up}$ is a Gosper form for g.

b. Let f be a hypergeometric term and $p, q, r \in C[x]$ be such that $\frac{\sigma(p)q}{p\sigma(r)}$ is a Gosper form for f. Let $u \in C[x]$ and $g = uf$. Show that $\frac{\sigma(up)q}{(up)\sigma(r)}$ is a Gosper form for g.

18⋆. Let $p, q, r \in C[x]$ be such that $u = \frac{q}{r} + \frac{p'}{p}$ is a Gosper form. Show that for every squarefree $t \in C[x]$ with $\gcd(r, t) = 1$, also $u = \frac{qt - rt'}{rt} + \frac{(pt)'}{pt}$ is a Gosper form.

19. Let h be a hypergeometric term. Prove or disprove:

a. If h is a kernel in the sense of Definition 2.72, then h has a Gosper form with $p = 1$.

b. If h has a Gosper form with $p = 1$, then h is a kernel in the sense of Definition 2.72.

20. Simplify the following sums.

a. $\sum_{k=0}^{n} \frac{3k+1}{k+1}\binom{2k}{k}$; **b.** $\sum_{k=0}^{n}(k+1)(23k+6)\binom{3k}{2k}$;

c. $\sum_{k=0}^{n} \frac{2x}{1+k-x}\binom{k}{k-x}\binom{k+x}{k}$ $(x \in \mathbb{Z} \setminus \{0\})$; **d.** $\sum_{k=0}^{n} \frac{4k+3}{2k+1}(-4)^k\binom{2k}{k}^{-1}$.

21⋆⋆. Under which circumstances can the Gosper equation have more than one solution? If this happens, how is this ambiguity reflected in the output?

22⋆. Find a polynomial $p \in C[x]$ of minimal degree such that $\sum_{k=0}^{n} p(k)/k!$ can be evaluated in closed form.

23. Gosper's algorithm is not limited to hypergeometric terms over $C(x)$ but applies, for example, also to hypergeometric terms over $C(q^x)$. Use it to evaluate the following indefinite sums involving the q-binomial coefficient $\binom{n}{k}_q$, which is defined through the equations

$$(q^k - q^{n+1})\binom{n+1}{k}_q + (q^{n+k+1} - q^k)\binom{n}{k}_q = 0,$$

$$(q^{2k+1} - q^k)\binom{n}{k+1}_q + (q^k - q^n)\binom{n}{k}_q = 0,$$

and the initial value $\binom{0}{0}_q = 1$.

a. $\sum_{k=1}^{n} \frac{q^{3k+3}+q^{2k+2}-q-1)q^k}{(1-q^{k+1})(1-q^{k+2})} \binom{2k}{k}_q$; **b.** $\sum_{k=1}^{n} (q^{2k+1}+q^k-1)(1-q^{3k+2})q^{k^2} \binom{2k}{k}_q$;

c. $\sum_{k=0}^{n} (q^{k+1} - 1)q^{\binom{k}{2}}$; **d.** $\sum_{k=1}^{n} \frac{q^k(q^{2k+1}+q^{k+1}-2)}{(1-q^k)(1-q^{2k+1})} \binom{2k}{k}_q^{-1}$.

24. Let $x \colon \mathbb{Z} \to C$ be any function with $x(n) \neq 0$ for all $n \in \mathbb{Z}$. For arbitrary $a \in \mathbb{Z}$, simplify the following sum:

$$\sum_{k=0}^{n} (-1)^k (x(k) + x(a-k)) \prod_{i=1}^{k} \frac{x(a-i+1)}{x(i)}.$$

25. The complete elliptic integral $K(x)$ satisfies the equation

$$K(x) + 4(2x-1)K'(x) + 4x(x-1)K''(x) = 0.$$

Simplify the following integrals involving $K(x)$:

a. $\int \frac{32-70x+41x^2+9x^3}{4(x-1)^2x^3} K(x)dx$;

b. $\int \frac{x(9x^2+7)}{(x^2-1)^3} K(x^2)dx$;

c. $\int \frac{12350x^5+1125x^4+341x-158}{(x-1)^4x^4} K(x)^2dx$.

26. The harmonic numbers $H_n = \sum_{k=1}^{n} \frac{1}{k}$ satisfy the recurrence

$$(n+2)H_{n+2} - (2n+3)H_{n+1} + (n+1)H_n = 0.$$

Simplify the following sums involving H_k:

a. $\sum_{k=1}^{n} H_k$; **b.** $\sum_{k=1}^{n} (10 + 24k + 9k^2)\binom{2k}{k} H_k$; **c.** $\sum_{k=1}^{n} kH_k^2$.

27. The discussion before Proposition 5.10 leads to the inhomogeneous equation $L^* \cdot v = -1$, but Proposition 5.10 itself states the equation $L^* \cdot v = 1$. Is this a typo?

28. Proposition 5.10 deals with the situation where we know an annihilating operator $L \in K[\Delta]$ of the summand/integrand. Show the following slight generalization to summands/integrands of the form pf for some $p \in K \setminus \{0\}$ and f is a function for which an annihilating operator $L \in K[\Delta]$ is given: There is an operator $Q \in K[\Delta]$ such that $\operatorname{rrem}(\Delta Q - p, L) = 0$ if and only if there is a $v \in K$ such that $L^* \cdot v = -p$.

29. The Motzkin numbers M_n satisfy the recurrence

$$3(n+1)M_n + (2n+5)M_{n+1} - (n+4)M_{n+2} = 0.$$

Find a polynomial $p \in C[x]$ such that the indefinite sum $\sum_{k=0}^{n} p(k)M_k$ can be expressed in terms of M_n and M_{n+1}.

30. Show that the dilogarithm $\mathrm{Li}_2(x) = \int_0^x \frac{\log(1-t)}{t} dt$ has no annihilating operator $L \in C(x)[D]$ of order two.

31. Suppose that f is a hypergeometric term for which the equation $\sigma(g) - g = f$ has a hypergeometric solution g. Let $L = uS - v \in C(x)[S]$ be an annihilating operator of f and let $p, q, r \in C[x]$ be such that $\frac{\sigma(p)}{p} \frac{q}{\sigma(r)}$ is a Gosper form of u/v. Express the solution $m \in C(x)$ of the adjoint equation $L^* \cdot m = -1$ in terms of p, q, r and the solution y of the Gosper equation.

32. Let $L \in K[\Delta]$. An element $v \in K$ is called an *integrating factor* of L if there exists a $Q \in K[\Delta]$ such that $vL = \Delta Q$. Show that $v \in K$ is an integrating factor for L if and only if $L^* \cdot v = 0$.

References

Hermite presented Hermite reduction in 1872 [236], apparently unaware that essentially the same method was already formulated a few decades earlier by Ostrogradsky [345, 346], who also introduced the alternative method sketched in Exercise 2. The Rothstein-Trager resultant appears in [375, 425]. Bronstein's book on symbolic integration [114] covers all these and some further techniques related to rational integration, including an algorithm by Czichowski [168] for finding the logarithmic part using Gröbner bases and an algorithm by Rioboo [368] which produces a logarithmic part without discontinuities.

The combination of Hermite reduction and the Rothstein-Trager resultant has been generalized to larger function classes. Trager [426] presents an integration algorithm of this kind for algebraic functions. Also the celebrated Risch algorithm [369, 370] for integration of elementary functions has this form. A compact introduction to Risch's algorithm can be found in the book of Geddes, Czapor, Labahn [206]. Bronstein's book [114] discusses it in full detail.

Gosper found his algorithm while he worked for the computer algebra system Macsyma. It was published in [221] at the recommendation of Knuth, who in the first edition of the first volume [279] of his classical textbook series *The Art of Computer Programming* had posed it as a research problem to develop computer programs for simplifying binomial sums. The integration analog of Gosper's algorithm appears in [30]. A few years before Gosper found his algorithm for indefinite hypergeometric summation, Abramov [2] had given an algorithm for indefinite rational summation. Abramov's algorithm for finding rational function solutions of linear recurrence equations with polynomial coefficients (Algorithm 2.64) is a generalization of his summation algorithm. Gerhard et al. [209] show that it can be decided in polynomial time whether the indefinite sum of a given rational function is rational. In his Ph.D. thesis [208], Gerhard analyzes the complexity of various algorithms related to rational and hyperexponential integration and hypergeometric summation, including algorithms based on homomorphic images.

There are also indefinite summation algorithms for larger classes. In the 1980s, Karr [258, 259] introduced an algorithm which can be viewed as a summation analog of Risch's integration algorithm. Roughly speaking, it can simplify expressions involving indefinite nested sums and products. For example, it can handle the simplifications requested in Exercise 26. The work of Karr was vastly extended into various directions by Schneider [384, 386, 388, 389, 391, 393–396].

Algorithm 5.8 is from [155]. The more special case that can be handled via adjoints is worked out in [10]. Observe that it can happen that the integral of a function f annihilated by some operator $L \in K[D_x]$ is not of the form $M \cdot f$ for some $M \in K[D_x]$ but nevertheless admits a nice closed form of some other type. A simple example in the case $K = C$ is given by the function $f(x) = x$, which is annihilated by $L = D_x^2$. We have $\int f(x)dx = \frac{1}{2}x^2$, but $\frac{1}{2}x^2$ is not of the form $M \cdot x$ for any $M \in C[D_x]$. In view of this example, we could ask more generally whether the integral of a function f annihilated by some operator $L \in K[D_x]$ can be expressed as rational function with coefficients in K of f and its derivatives, rather than just as a K-linear combination of f and its derivatives. For the differential case, this question is addressed by Bertrand [60].

5.2 The Definite Problem

The fundamental theorem of calculus relates indefinite to definite integration. It says that

$$\int_a^b f(x)dx = g(b) - g(a)$$

if $g = \int f$ is an indefinite integral of f. There are two main issues with the application of this theorem. The first is that a simple expression for a definite integral may exist even if the corresponding indefinite integral cannot be expressed in closed form. The standard example is $\int_{-\infty}^{\infty} \mathrm{e}^{-x^2} dx = \sqrt{\pi}$. The second issue is that the fundamental theorem of calculus requires f and g to be continuous in the range of integration. For example, for $f(x) = \frac{1}{1+x^2}$ we have $\int f(x)dx = -\arctan(1/x) =: g(x)$, because

$$g'(x) = -\arctan(1/x)' = -\frac{1}{1+1/x^2}\Bigl(-\frac{1}{x^2}\Bigr) = \frac{1}{1+x^2} = f(x),$$

however,

$$\int_{-1}^{1} f(x)dx = \frac{\pi}{2} \neq -\frac{\pi}{2} = g(1) - g(-1).$$

Observe that in this example, only the antiderivative g has a singularity in the integration range while the integrand f is perfectly well-behaved.

Both issues cause serious trouble in the development of computer algebra algorithms for evaluating definite sums and integrals. For neither do we have a satisfactory algorithmic solution. Although developers of general purpose computer algebra systems work hard to ensure that their code succeeds in evaluating definite sums and integrals correctly, the output of a general purpose simplifier for definite sums or integrals should be handled with a healthy portion of distrust.

At the same time, computer algebra provides valuable tools with which astonishing results about definite sums and integrals have been proven, and it is worth knowing how these tools work, how they are applied, what they are capable of, and also which responsibilities they leave to the user. These questions will occupy us for the remainder of this book.

One aspect shared by the algorithms to come is that they only apply to definite sums and integrals involving at least one free parameter, i.e., at least one additional variable besides the variable over which we want to sum or integrate. Consequently, the definite sums and integrals we consider are not just certain numbers, but they are functions in these free variables, and what we want to compute are annihilating operators for these functions.

Example 5.12

1. The Gamma function can be defined as $\Gamma(z) := \int_0^\infty x^{z-1}\mathrm{e}^{-x}dx$ for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 0$. The first order recurrence $\Gamma(z+1) = z\Gamma(z)$ follows from the relation

$$-zf(x,z) + f(x,z+1) + \frac{d}{dx}f(x,z+1) = 0$$

satisfied by the integrand $f(x,z) = x^{z-1}\mathrm{e}^{-x}$. Indeed, integrating this relation for x from 0 to ∞ gives

$$-z\Gamma(z) + \Gamma(z+1) + \underbrace{\big[f(x,z+1)\big]_{x=0}^{\infty}}_{=0} = 0$$

which is equivalent to the desired recurrence $\Gamma(z+1) = z\Gamma(z)$.

2. Consider the definite sum $f(n) = \sum_k \binom{n}{k}$ for $n \geq 0$. According to the binomial theorem we have $f(n) = 2^n$, so there is a recurrence $f(n+1) - 2f(n) = 0$. This recurrence follows from the Pascal triangle recurrence

$$\binom{n+1}{k+1} - \binom{n}{k} - \binom{n}{k+1} = 0 \qquad (n \in \mathbb{N}, k \in \mathbb{Z}),$$

because summing this equation over all k gives

$$\sum_k \binom{n+1}{k+1} - \sum_k \binom{n}{k} - \sum_k \binom{n}{k+1} = 0,$$

which is equivalent to the desired recurrence $f(n+1) - 2f(n) = 0$.

Observe that there is an unfortunate and possibly confusing notational inconsistency: while an integral expression without explicitly stated bounds, like $\int f(x)dx$, refers to an indefinite integral, a sum expression without explicitly stated bounds, like $\sum_k f(k)$, is typically understood as a sum ranging over all integers, i.e., $\sum_k f(k) = \sum_{k=-\infty}^{\infty} f(k)$, and is thus a definite sum.

□

The relations of the summand/integrand in these examples translate easily into relations for the sum/integral because their coefficients do not involve the summation/integration variable. This observation raises three questions:

1. Do linear relations whose coefficients are free of the summation/integration variable always exist?
2. Does every such relation translate into a nontrivial relation for the corresponding definite sum/integral?
3. Are the resulting linear relations for the definite sum/integral always homogeneous?

The answer to all three questions is "not quite."

For the first question, instead of assuming that the summand/integrand is D-finite, it is more appropriate to assume that it is holonomic. Indeed, it follows directly from Definition 4.67 that if $I \subseteq C[x,t][\partial_x, \partial_t]$ is a holonomic left ideal, then $I \cap C[t][\partial_x, \partial_t]$ contains a nonzero operator. According to Theorem 4.69, D-finiteness and holonomy are essentially the same in the differential case, so at least here we do not need to worry too much. In the shift case however, the relation between D-finiteness and holonomy is more subtle. Classical summation theory, which focuses on sums over hypergeometric terms, imposes certain restrictions on the shape of summands in order to ensure the existence of relations of the desired form.

Definition 5.13 A bivariate hypergeometric term h is called *proper* if there are $p \in C[n,k]$, $\phi, \psi \in C$, $M \in \mathbb{N}$, and $a_m, a'_m, e_m \in \mathbb{Z}$, $a''_m \in C$ $(m = 1, \ldots, M)$ such that h can be written as

$$h = p(n,k)\phi^n \psi^k \prod_{m=1}^{M} \Gamma(a_m n + a'_m k + a''_m)^{e_m}.$$

□

For example, $\binom{n}{k}$ can be written as $\Gamma(n+1)\Gamma(k+1)^{-1}\Gamma(n-k+1)^{-1}$ and is thus a proper hypergeometric term, but $\frac{1}{n^2+k^2}$, while hypergeometric, is not proper hypergeometric.

Theorem 5.14 *Every proper hypergeometric term is holonomic.* □

Proof Let h be a proper hypergeometric term. Since h is hypergeometric, it is clear that it has nonzero annihilating operators in $C[n,k][S_n]$ and $C[n,k][S_k]$, respectively. We have to show that it also has nonzero annihilating operators in $C[n][S_n, S_k]$ and $C[k][S_n, S_k]$, respectively. As the definition is symmetric with respect to n and k, it suffices to show that there is a nonzero annihilating operator in $C[n][S_n, S_k]$.

The idea is to choose some $r \in \mathbb{N}$ and make an ansatz $L = \sum_{i=0}^{r} \sum_{j=0}^{r} \ell_{i,j} S_n^i S_k^j$ for undetermined $\ell_{i,j} \in C[n]$, and then to show that for sufficiently large r the linear system resulting from equating $L \cdot h$ to zero has more variables than equations. For describing this linear system it is useful to separate positive and negative a'_m's as well as positive and negative e_m's. Let us therefore write h in the form

$$h = p(n,k)\phi^n \psi^k \prod_{m=1}^{M} \frac{\Gamma(a_m n + a'_m k + a''_m)\Gamma(b_m n - b'_m k + b''_m)}{\Gamma(u_m n + u'_m k + u''_m)\Gamma(v_m n - v'_m k + v''_m)}$$

where now $a_m, a'_m, b_m, b'_m, u_m, u'_m, v_m, v'_m$ are assumed to be *nonnegative* integers, and not necessarily pairwise distinct. It is without loss of generality that we assume that there is the same number of gamma factors for each of the four indicated types, because we can always put further factors $\Gamma(0n + 0k + 1)$ into the product if necessary. It is also without loss of generality that we assume that there is no $\Gamma(wn + w'k + w'')$ with $w < 0$, because we can replace any such factor with $(-1)^{wn+w'k}\Gamma(-wn - w'k - w'' + 1)^{-1}$.

With the shorthand notations

$$\begin{aligned} A_m &= a_m n + a'_m k + a''_m, \quad & B_m &= b_m n - b'_m k + b''_m, \\ U_m &= u_m n + u'_m k + u''_m, \quad & V_m &= v_m n - v'_m k + v''_m, \end{aligned}$$

for $m = 1, \ldots, M$ and $q^{\overline{s}} = q(q+1)\cdots(q+s-1)$ for $q \in C[n,k]$ and $s \in \mathbb{N}$, we have

$$\begin{aligned} S_n \cdot \Gamma(A_m) &= A_m^{\overline{a_m}} \Gamma(A_m), \quad & S_k \cdot \Gamma(A_m) &= A_m^{\overline{a'_m}} \Gamma(A_m), \\ S_n \cdot \Gamma(B_m) &= B_m^{\overline{b_m}} \Gamma(B_m), \quad & S_k \cdot \Gamma(B_m) &= \frac{1}{(B_m - b'_m)^{\overline{b'_m}}} \Gamma(B_m), \\ S_n \cdot \Gamma(U_m) &= U_m^{\overline{u_m}} \Gamma(U_m), \quad & S_k \cdot \Gamma(U_m) &= U_m^{\overline{u'_m}} \Gamma(U_m), \\ S_n \cdot \Gamma(V_m) &= V_m^{\overline{v_m}} \Gamma(V_m), \quad & S_k \cdot \Gamma(V_m) &= \frac{1}{(V_m - v'_m)^{\overline{v'_m}}} \Gamma(V_m), \end{aligned}$$

for all m, and therefore

$$\frac{S_n^i S_k^j \cdot h}{h} = \phi^i \psi^j \frac{S_n^i S_k^j \cdot p}{p} \prod_{m=1}^{M} \frac{A_m^{\overline{ia_m + ja'_m}} B_m^{\overline{ib_m}} (V_m - jv'_m)^{\overline{jv'_m}}}{U_m^{\overline{iu_m + ju'_m}} V_m^{\overline{iv_m}} (B_m - jb'_m)^{\overline{jb'_m}}}$$

for all $i, j \in \mathbb{N}$. The polynomial

$$d = \prod_{m=1}^{M} U_m^{\overline{ru_m + ru'_m}} V_m^{\overline{rv_m}} (B_m - rb'_m)^{\overline{rb'_m}}$$

is a common denominator (not necessarily the least) of the rational function $(L \cdot h)/h$. Its degree in k is $r \sum_{m=1}^{M} (u_m + u'_m + v_m + b'_m)$, and the numerator of $d(L \cdot h)/h$ is a polynomial whose degree in k is bounded by

$$\deg_k(p) + r \sum_{m=1}^{M} \left(a_m + a'_m + b_m + b'_m + u_m + u'_m + v_m + v'_m\right) = \mathrm{O}(r).$$

As the ansatz for L contains $(r+1)^2$ undetermined coefficients $\ell_{i,j}$ and equating the coefficients of the polynomial $d(L \cdot h)/h$ to zero only leads to $\mathrm{O}(r)$ equations, it follows that for sufficiently large r there will be more variables than equations and therefore a nontrivial solution. ■

The proofs of Theorems 5.14 and 4.69 share the same key observation: the normal forms of many (here: quadratically many) operator monomials have a relatively small (here: linear size) common denominator, and the resulting gap leads to the desired underdetermined linear system. In Theorem 4.69 the smallness of the common denominator was ensured by the assumption that all σ's of the Ore algebra are equal to id. This is not the case in Theorem 5.14. Here, the common denominator stays small because the factors contributed by shifts in n and the factors contributed by shifts in k have a significant overlap. For example, we have

$$\begin{aligned} S_k \cdot \Gamma(3n + 2k) &= \underbrace{(3n + 2k)(3n + 2k + 1)}_{=}\,\Gamma(3n + 2k), \\ S_n \cdot \Gamma(3n + 2k) &= \overbrace{(3n + 2k)(3n + 2k + 1)}(3n + 2k + 2)\Gamma(3n + 2k). \end{aligned}$$

The proof of Theorem 5.14 is easily translated into an algorithm that computes for any given proper hypergeometric term a linear recurrence whose polynomial coefficients are free of k.

Example 5.15

1. Consider $h = \binom{n}{k}$. With the ansatz $L = \ell_{0,0} + \ell_{1,0} S_n + \ell_{0,1} S_k + \ell_{1,1} S_n S_k$ we have

$$\begin{aligned}\frac{L \cdot h}{h} &= \ell_{0,0} + \ell_{1,0}\frac{n+1}{n-k+1} + \ell_{0,1}\frac{n-k}{k+1} + \ell_{1,1}\frac{n+1}{k+1} \\ &= \Big(\ell_{0,0}(k+1)(k-n-1) - \ell_{0,1}(k-n-1)(k-n) \\ &\qquad -\ell_{1,0}(k+1)(n+1) + \ell_{1,1}(n+1)(k-n-1)\Big)\Big/\Big((k+1)(k-n-1)\Big).\end{aligned}$$

Equating coefficients of k^0, k^1, k^2 of the numerator to zero gives the linear system

$$\begin{pmatrix} -n-1 & -n-1 & -n(n+1) & -(n+1)^2 \\ -n & -n-1 & 2n+1 & n+1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} \ell_{0,0} \\ \ell_{1,0} \\ \ell_{0,1} \\ \ell_{1,1} \end{pmatrix} = 0.$$

The solution space is generated by the vector $(-1, 0, -1, 1)$, which corresponds to the operator $L = S_n S_k - S_k - 1$, which in turn corresponds to the Pascal triangle recurrence for the binomial coefficients.

2. In the differential case we can proceed analogously. For $h = x^{z-1}\mathrm{e}^{-x}$ we have $(S_z \cdot h)/h = x$ and $(D_x \cdot h)/h = (z - x - 1)/x$. With the ansatz $L = \ell_{0,0} + \ell_{1,0}S_z + \ell_{0,1}D_x + \ell_{1,1}S_z D_x$ we get

$$\begin{aligned}\frac{L \cdot h}{h} &= \ell_{0,0} + \ell_{1,0}x + \ell_{0,1}\frac{x+z-1}{x} + \ell_{1,1}(z-x) \\ &= \big(\ell_{0,0}x + \ell_{1,0}x^2 + \ell_{0,1}(x+z-1) + \ell_{1,1}(z-x)x\big)/x,\end{aligned}$$

and coefficient comparison gives a linear system with four variables and three equations. This system has a solution which translates to the operator $L = S_z D_x + S_z - z$, which matches the relation used in part 1 of Example 5.12. □

The ansatz $L = \sum_{i,j=0}^{r} \ell_{i,j} S_n^i S_k^j$ used in the proof of Theorem 5.14 is fine for the theoretical argument, but it is not the best choice in all situations. For example, we may prefer the resulting recurrence or differential equation for the definite sum/integral under consideration to have a low order. In view of this preference, we may want to use an ansatz which uses higher orders for the summation/integration variable, for instance $\sum_{i=0}^{r} \sum_{j=0}^{3r} \ell_{i,j} S_n^i S_k^j$. Another reason for adjusting the shape of the ansatz is to optimize the shape of the linear system: it may be possible to introduce additional variables without increasing the number of equations, i.e., the inclusion of some further terms $\ell_{i,j} S_n^i S_k^j$ to the ansatz may not affect the denominator or the degree of the numerator. Detecting and including such terms is known as *Verbaeten completion*. They can be identified using relations such as $S_n^{a'} \cdot \Gamma(an + a'k + a'') = S_k^{a} \cdot \Gamma(an + a'k + a'')$ $(a, a' > 0)$.

Example 5.16 Consider the hypergeometric term $h = \binom{a}{k}\binom{b}{n-k}$, where a and b are constant parameters. For the ansatz $L = \ell_{0,0} + \ell_{1,0}S_n + \ell_{0,1}S_k + \ell_{1,1}S_kS_n$ we have

$$\frac{L \cdot h}{h} = \frac{(\cdots) + (\cdots)k + (\cdots)k^2 + (\cdots)k^3}{(k+1)(k-n-1)(b+k-n+1)},$$

which leads to a linear system with four variables and four equations that turns out to have no nonzero solution. The observation

$$\frac{S_kS_n^2 \cdot h}{h} = \frac{(k-a)(b+k-n)}{(k+1)(k-n-1)} = \frac{(\cdots) + (\cdots)k + (\cdots)k^2 + (\cdots)k^3}{(k+1)(k-n-1)(b+k-n+1)}$$

indicates that adding the term $S_kS_n^2$ will still lead to a linear system with four equations, but now with five variables. This linear system has a solution which corresponds to the operator

$$L = (n-a-b) + (n-a+1)S_n + (n-b+1)S_kS_n + (n+2)S_kS_n^2.$$

Summing the relation $L \cdot h = 0$ over all $k \in \mathbb{Z}$ gives the correct annihilating operator $(n-a-b) + (2n+2-a-b)S_n + (n+2)S_n^2$ for the sum $\sum_k \binom{a}{k}\binom{b}{n-k}$. □

Gröbner bases provide an alternative way to find k-free recurrences. As outlined in Sect. 4.6, knowing generators of an ideal $I \subseteq C[n,k][S_n, S_k]$, we can use Buchberger's algorithm to find generators of the elimination ideal $I \cap C[n][S_n, S_k]$. In the example above, taking $I = \langle (n+1-k)S_n - (n-k-b), (k+1)(k+b+1-n)S_k + (a-k)(k-n)\rangle$ gives $I \cap C[n][S_n, S_k] = \langle L \rangle$ with L being the operator stated in the example. It should be noted however that the computation of the elimination ideal via Gröbner bases is not equivalent to the linear algebra approach described in Example 5.15.

Example 5.17 For the hypergeometric term $h = k^2\binom{n}{k}$, the linear algebra approach with the ansatz $L = \sum_{i=0}^{1}\sum_{j=0}^{2} \ell_{i,j}S_n^iS_k^j$ leads to the annihilating operator

$$L = (n+1)^2 + (n+1)(n+2)S_k + (n+1)S_k^2 - n^2S_kS_n - nS_k^2S_n,$$

which in turn implies $\bigl(2(n+1)(n+2) - n(n+1)S_n\bigr) \cdot \sum_k k^2\binom{n}{k} = 0$.

For the ideal $I = \langle k^2S_k + (k+1)(k-n), (n+1-k)S_n - (n+1)\rangle \subseteq C[n,k][S_n, S_k]$, a Gröbner basis computation finds

$$\begin{aligned} I \cap C[n][S_n, S_k] = \langle (1+n)^2S_n^2S_k - (2+n)(1+2n)S_nS_k \\ - (2+n)^2S_n + (1+n)(2+n)S_k + (1+n)(2+n)\rangle, \end{aligned}$$

and it may come as a surprise that this ideal does not contain the operator L. □

The technical reason for this discrepancy is that the linear algebra approach amounts to a search in an ideal of the algebra $C(n,k)[S_n,S_k]$ rather than $C[n,k][S_n,S_k]$, and while L is contained in the ideal generated by $k^2S_k+(k+1)(k-n)$ and $(n+1-k)S_n-(n+1)$ in $C(n,k)[S_n,S_k]$, it is not contained in the ideal generated by these operators in the smaller Ore algebra $C[n,k][S_n,S_k]$. In order to ensure that Gröbner bases find all elements that the linear algebra approach can find, we need to take $I=J\cap C[n,k][S_n,S_k]$, where J is the ideal generated by $S_k-\frac{(n-k)(k+1)}{k^2}$ and $S_n-\frac{n+1}{n+1-k}$ in $C(n,k)[S_n,S_k]$. This ideal I is called the *contraction ideal* of J. The computation of such contraction ideals is a difficult problem.

On the other hand, if we know generators of the annihilating ideal of a summand/integrand from some source, then a Gröbner basis computation provides somewhat more information than the linear algebra approach, in at least two respects. First, it finds not only some k-free operators but (a finite description of) all of them. Secondly, it is more robust against possible issues with singularities. For example, the computation

$$\begin{aligned}&\langle (k+1)S_k-(n-k),(n+1-k)S_n-(n+1)\rangle\cap C[n][S_n,S_k]\\&=\langle (n+1)S_nS_k-(n+1)S_k-(n+1)\rangle\end{aligned}$$

leads to the recurrence equation $\bigl((n+1)S_n-2(n+1)\bigr)\cdot\sum_{k=0}^n\binom{n}{k}=0$, which holds not only for all $n\in\mathbb{N}$ but in fact for all $n\in\mathbb{Z}$.

Regardless of whether we use Gröbner bases or linear algebra to find a linear relation for the summand/integrand whose coefficients do not involve the summation/integration variable, we now know that such relations exist at least for holonomic functions. The question remains under which circumstances such a linear relation can be translated into linear recurrence/differential equation for the sum/integral. To see that not all relations are useful, observe that the binomial coefficient also satisfies the relation

$$\binom{n}{k}-\binom{n}{k+2}-\binom{n+1}{k+1}+\binom{n+1}{k+2}=0\qquad(n\in\mathbb{N},k\in\mathbb{Z}),$$

and summing this relation over all integers k leads to the conclusion $0=0$, which fails to provide any useful information about the sum $\sum_k\binom{n}{k}$. The problem can be fixed by adjusting the relations a bit. For doing so, let us rephrase the problem in operator language.

Suppose we are given an ideal I of $C(x,t)[\partial_x,\partial_t]$ or $C[x,t][\partial_x,\partial_t]$ of annihilating operators for a function f that we want to sum/integrate with respect to x. Suppose that ∂_x acts as a derivation or a forward difference, respectively. Let L be a nonzero element of $I\cap C(t)[\partial_x,\partial_t]$, or $C[t][\partial_x,\partial_t]$, respectively. The effect of summing/integrating over a relation $L\cdot f=0$ becomes more clear if we write

$L = P - \partial_x Q$ for certain operators P, Q that are free of x. We can always produce such a decomposition by left-division with remainder. Since P does not involve x or ∂_x, it is fair to assume that summation/integration with respect to x commutes with P. Furthermore, summation/integration of $\partial_x Q \cdot f$ yields the difference of two evaluations of $Q \cdot f$ by the fundamental theorem of calculus, or its discrete counterpart. More precisely, the definite integral $F(t) = \int_a^b f(x,t)dx$ or the definite sum $F(t) = \sum_{x=a}^{b-1} f(x,t)$ satisfies the relation

$$(P \cdot F)(t) = (Q \cdot f)(b,t) - (Q \cdot f)(a,t).$$

The left hand side is critical: we obtain a nontrivial relation for the sum/integral F if and only if the operator P is nonzero.

Definition 5.18 Let $I \subseteq C(x,t)[\partial_x, \partial_t]$. An operator $P \in C(t)[\partial_t]$ is called a *telescoper* for I if there exists a $Q \in C(x,t)[\partial_x, \partial_t]$ such that $P - \partial_x Q \in I$. In this case, such a Q is called a *certificate* for P. If I is a set of annihilating operators of some function f, we may also say that P is a telescoper for f. □

Note that while Q may contain x and may be zero, P must not contain x and is only useful if it is nonzero. If P is zero, it is not useful because summing/integrating over a relation $(0 - \partial_x Q) \cdot f = 0$ does not provide us with any information about the sum/integral under consideration but only yields the degenerate equation $0 = 0$. Fortunately, using the freedom that x may appear in Q, we can turn an annihilating operator $\partial_x Q$ for f into an annihilating operator $P_0 - \partial_x Q_0$ with P_0 nonzero and free of x. The following lemma is the key.

Lemma 5.19 *(Wegschaider) Let $A = R[\partial]$ be an Ore algebra and write $\sigma^{\overline{k}}(p) = p\sigma(p)\cdots\sigma^{k-1}(p)$ for $k \in \mathbb{N}$ and $p \in R$. Let $p \in R$ be such that $\delta(\sigma^i(p) + \cdots + \sigma^j(p))$ is a constant for all $i, j \in \mathbb{Z}$ with $i \leq j$. Then for every $k \in \mathbb{N}$ there exists an $M \in R[\partial]$ such that*

$$\sigma^{\overline{k}}(p)\partial^k = \partial M + (-1)^k \prod_{i=0}^{k-1} \sum_{j=0}^{i} \delta(\sigma^{j-1}(p)).$$

□

Proof Recall from Exercise 4 of Sect. 4.1 that we have

$$\delta(\sigma^{\overline{k}}(p)) = \sigma^{\overline{k-1}}(\sigma(p)) \sum_{j=0}^{k-1} \delta(\sigma^j(p))$$

for all $k \in \mathbb{N}$. Using this formula and the commutation rule $\partial u = \sigma(u)\partial + \delta(u)$ $(u \in R)$, we can prove the claim by induction on k. For $k = 0$ the statement is $1 = 1$, which is true. If it is true for a certain k, then

$$
\begin{aligned}
&\sigma^{\overline{k+1}}(p)\partial^{k+1} \\
&= \Big(\partial\, \sigma^{\overline{k+1}}(\sigma^{-1}(p)) - \delta\big(\sigma^{\overline{k+1}}(\sigma^{-1}(p))\big)\Big)\partial^k \\
&= \partial\, \sigma^{\overline{k+1}}(\sigma^{-1}(p))\partial^k - \Big(\sum_{j=0}^{k} \delta(\sigma^{j-1}(p))\Big)\sigma^{\overline{k}}(p)\partial^k \\
&= \partial\, \sigma^{\overline{k+1}}(\sigma^{-1}(p))\partial^k - \Big(\sum_{j=0}^{k} \delta(\sigma^{j-1}(p))\Big)\Big(\partial M + (-1)^k \prod_{i=0}^{k-1}\sum_{j=0}^{i} \delta(\sigma^{j-1}(p))\Big) \\
&= \partial\sigma^{\overline{k+1}}(\sigma^{-1}(p))\partial^k - \underbrace{\sum_{j=0}^{k} \delta(\sigma^{j-1}(p))\partial M}_{= \Big(\partial \sum_{j=0}^{k} \delta(\sigma^{j-2}(p)) - \delta\big(\sum_{j=0}^{k} \delta(\sigma^{j-2}(p))\big)\Big) M} + (-1)^{k+1} \prod_{i=0}^{k}\sum_{j=0}^{i} \delta(\sigma^{j-1}(p)) \\
&= \partial\Big(\sigma^{\overline{k+1}}(\sigma^{-1}(p))\partial^k - \sum_{j=0}^{k} \delta(\sigma^{j-2}(p))M\Big) + (-1)^{k+1} \prod_{i=0}^{k}\sum_{j=0}^{i} \delta(\sigma^{j-1}(p)),
\end{aligned}
$$

because $\delta\big(\sum_{j=0}^{k} \delta(\sigma^{j-2}(p))\big) = 0$ by assumption. ■

In our context, the lemma is applied with $R = C[x,t][\partial_t]$ or $R = C(x,t)[\partial_t]$ and $p = x$. Note that if ∂_x acts as a derivation or as a difference operator, then $\delta_x(x) = 1$, so $\delta_x(\sigma_x^i(x) + \cdots + \sigma_x^j(x)) = j + 1 - i$ is a constant, as the lemma requires. As the constant is different from zero whenever $i \leq j$, it follows that the product $c := \prod_{i=0}^{k-1}\sum_{j=0}^{i} \delta(\sigma^{j-1}(x)) = \prod_{i=0}^{k-1} \delta\big(\sum_{j=0}^{i} \sigma^{j-1}(x)\big)$ is a nonzero constant. This is what we will exploit. If a nonzero element L of the elimination ideal $I \cap C[t][\partial_x, \partial_t]$ is a right-multiple of ∂_x, so that $P = 0$, we let $k \in N$ be maximal such that $L = \partial_x^k L_0$ for some $L_0 \in C[x,t][\partial_x, \partial_t]$. By the lemma, we then have

$$\sigma^{\overline{k}}(x)L = \sigma^{\overline{k}}(x)\partial_x^k L_0 = \partial_x M + cL_0$$

for $c = (-1)^k \prod_{i=0}^{k-1}\sum_{j=0}^{i} \delta(\sigma^{j-1}(x)) \neq 0$ and some $M \in C[x,t][\partial_x, \partial_t]$. Since L_0 is not a right-multiple of ∂_x by the choice of k, we can write it as $L_0 = P_0 - \partial_x Q_0$ for some nonzero $P_0 \in C[t][\partial_t]$ and some $Q_0 \in C[t][\partial_x, \partial_t]$ and obtain

$$\sigma^{\overline{k}}(x)L = cP_0 + \partial_x(M + cQ_0).$$

If L is an annihilating operator of the summand/integrand, then so is $\sigma^{\overline{k}}(x)L$, and since cP_0 is not the zero operator, summing/integrating over the relation $\sigma^{\overline{k}}(x)L \cdot f = 0$ is bound to yield a nontrivial relation for the sum/integral.

Example 5.20 The relation

$$\binom{n}{k} - \binom{n}{k+2} - \binom{n+1}{k+1} + \binom{n+1}{k+2} = 0$$

amounts to the operator $1 - S_k^2 - S_n S_k + S_n S_k^2 \in C[k,n][S_k, S_n]$. In the discussion above it is assumed that the Ore algebra generator ∂_x corresponding to the summation/integration variable acts as a derivation or difference operator, respectively, but not as a shift. We therefore translate the operator to $-2\Delta_k - \Delta_k^2 + \Delta_k S_n + \Delta_k^2 S_n$ and see that it factorizes as $\Delta_k L_0$ with $L_0 = -2 - \Delta_k + S_n + \Delta_k S_n$. Using $k\Delta_k = \Delta_k k - 1$ we get

$$k\Delta_k L_0 = \Delta_k k L_0 - L_0 = \Delta_k(kL_0 + 1 + S_n) - (S_n - 2).$$

Summing the relation $k\Delta_k L_0 \cdot \binom{n}{k} = 0$ over all k yields the annihilating operator $S_n - 2$ of $\sum_k \binom{n}{k}$, as expected. □

The term telescoper originates from classical hypergeometric summation theory. Here we say that a hypergeometric term h telescopes if the equation $\sigma(g) - g = h$ has a hypergeometric solution. This is exactly the problem of indefinite summation discussed in the previous section. According to Definition 5.18, an operator P is a telescoper for h if $P \cdot h$ telescopes. Indeed, if Q is a certificate for P, then $g = Q \cdot h$ is such that $\sigma(g) - g = P \cdot h$.

The term certificate was chosen for Q because if we know Q, then checking whether P is a telescoper amounts to checking whether $P - \partial_x Q$ annihilates the summand/integrand, which at least in the case of hypergeometric terms is a straightforward thing to do. If we do not know Q, it is more difficult to check whether P is really a telescoper or not. So Q certifies that P is indeed a telescoper.

In general, the certificate is also needed in the derivation of the equation for the definite sum/integral. Recall that $(P - \partial_x Q) \cdot f = 0$ implies the relation

$$(P \cdot F)(t) = (Q \cdot f)(b,t) - (Q \cdot f)(a,t)$$

for the definite integral $F(t) = \int_a^b f(x,t)dx$ or the definite sum $F(t) = \sum_{x=a}^{b-1} f(x,t)$. In all examples we have seen so far, the right hand side turned out to be zero. This is often the case, but not always.

Example 5.21

1. For $f(x,t) = \frac{1}{1+x^2+t^2}$ consider $F(t) = \int_0^1 f(x,t)dx$. We have $((1+t^2)D_t + t - D_x(tx)) \cdot f(x,t) = 0$, so $P = (1+t^2)D_t + t$ is a telescoper for f and

$Q = tx$ is a certificate for P. Integrating $(P - D_x Q) \cdot f = 0$ from 0 to 1 gives the inhomogeneous differential equation

$$P \cdot F = \left[\frac{xt}{1 + x^2 + t^2}\right]_{x=0}^{1} = \frac{t}{t^2 + 2}$$

for the definite integral. Applying $(t^2 + 2)tD_t + (t^2 - 2)$ to both sides in order to annihilate the right hand side, we find that

$$\big((t^2+2)tD_t+(t^2-2)\big)\big((1+t^2)D_t+t\big)=t(t^2+1)(t^2+2)D_t^2+(4t^4+5t^2-2)D_t+2t^3$$

is an annihilating operator for F.

2. For $f(n,k) = \binom{2n}{k}$ consider $F(n) = \sum_{k=0}^{n} f(n,k)$. We have

$$\big((S_n - 4) - (S_k - 1)(3 + S_k - S_n - S_k S_n)\big) \cdot f = 0,$$

so $P = S_n - 4$ is a telescoper for f and $Q = 3 + S_k - S_n - S_k S_n$ is a certificate for P.
If we apply the summation $\sum_{k=0}^{n}$ to the relation $(P - \Delta_k Q) \cdot f = 0$, we have to observe that an additional term needs to be added in order to complete $\sum_{k=0}^{n} f(n+1,k)$ to $F(n)$. Since the term has to be added on both sides in order to maintain the equality, it also contributes to the inhomogeneous part of the resulting equation:

$$\underbrace{\sum_{k=0}^{n}\binom{2n+2}{k} + \binom{2n+2}{n+1}}_{=F(n+1)} - 4\underbrace{\sum_{k=0}^{n}\binom{2n}{k}}_{=F(n)} = \binom{2n+2}{n+1} + \left[Q \cdot \binom{2n}{k}\right]_{k=0}^{n+1}$$
$$= -\frac{1}{n+1}\binom{2n}{n}.$$

Applying $(n+2)S_n - (4n+2)$ in order to annihilate the right hand side, we find that

$$\big((n+2)S_n - (4n+2)\big)(S_n - 4) = (n+2)S_n^2 - (8n+10)S_n + (16n+8)$$

is an annihilating operator for the sum F.

3. Let $f(n,x) = P_n(x)^2$ be the squared nth Legendre polynomial and consider the definite integral $F(n) = \int_0^1 f(n,x)dx$. We have

$$\big((2n+3)S_n - (2n+1) - D_x(\tfrac{x^2+1}{n+1}D_x - xS_n + x)\big) \cdot f = 0,$$

so $P = (2n+3)S_n - (2n+1)$ is a telescoper for f and $Q = \frac{x^2+1}{n+1} D_x - xS_n + x$ is a certificate for P.

Integrating the relation $(P - D_x Q) \cdot f = 0$ gives

$$(2n+3)F(n+1) - (2n+1)F(n) = \Big[Q \cdot P_n(x)^2\Big]_{x=0}^{1} = -P_n(0)P_{n+1}(0).$$

In this case, an annihilating operator for the right hand side is $(n+2)S_n^2 - (n+1)$ (cf. Exercise 15), so we obtain the annihilating operator

$$\begin{aligned}&\big((2n+3)S_n^2 - (2n+1)\big)\big((2n+3)S_n - (2n+1)\big)\\ &= (3+n)(7+2n)S_n^3 - (3+n)(5+2n)S_n^2 - (1+n)(3+2n)S_n + (1+n)(1+2n)\end{aligned}$$

for the definite integral.

□

In many examples arising from applications, the right hand side $[Q \cdot f]_{x=a}^{b}$ evaluates to zero, so the telescoper P itself is already an annihilating operator of the sum/integral. In some cases the collapsing of the right hand side to zero looks like a lucky coincidence. In other cases the collapsing is less surprising. The following definition tries to capture this latter situation.

Definition 5.22 A definite sum/integral of a function f over a domain Ω is said to have *natural boundaries* if the sum/integral over Ω of $\partial_x Q \cdot f$ is zero for all operators Q that are certificates for some telescoper for f. □

This definition is informal in so far as we do not specify where the Q live. In view of possible issues with singularities in the summation/integration range, it might make a difference whether we consider telescopers with certificates in $C(x,t)[\partial_x, \partial_t]$ or in $C[x,t][\partial_x, \partial_t]$. The intended reading of Definition 5.22 is relative to the choice of the Ore algebra.

With respect to the algebra $C[n,k][S_n, S_k]$, it is often easy to recognize by inspection that a definite hypergeometric sum has natural boundaries. For example, for every fixed $n \in \mathbb{N}$ we have $\binom{n}{k} = 0$ for all $k < 0$ and all $k > n$, and as the application of an operator $Q \in C[n,k][S_n, S_k]$ amounts to a multiplication with a certain rational function, we also have $\lim_{|k|\to\infty} Q \cdot \binom{n}{k} = 0$ for every fixed $n \in \mathbb{N}$ and every $Q \in C[n,k][S_n, S_k]$ for which $Q \cdot \binom{n}{k}$ is well defined. This observation suffices to conclude that the definite sum $\sum_k \binom{n}{k}$ has natural boundaries.

Natural boundaries also appear naturally for contour integrals. If γ is a closed path in the complex plane and f is a holonomic function in x and t which is such that for every fixed t the univariate function $x \mapsto f(x,t)$ has no singularity on the path γ, then $\oint_\gamma D_x Q \cdot f(x,y)\,dx = 0$ for all $Q \in C(x,t)[D_x, D_t]$.

A definite sum/integral with natural boundaries over a bivariate summand/integrand depends on a single variable. Since we have shown that every holonomic summand/integrand admits a nonzero telescoper, and the assumption of natural boundaries allows us to conclude that any such telescoper annihilates the sum/integral, it follows that the sum/integral is holonomic as a univariate function. We have thus found a new closure property: definite summation/integration with natural boundaries preserves holonomy.

This feature extends to the case of more variables. We can allow several free variables as well as several summation/integration variables. The case of several summation/integration variables applies to definite nested sums/integrals, which also may be mixed. The techniques discussed so far admit straightforward generalizations to this setting. Also the terminology of telescopers and certificates and natural boundaries is extended to the case of several variables. Note that in this more general situation, the certificate of a telescoper is a tuple of operators.

Example 5.23 The hypergeometric term $f(n,k,i,j) = \binom{n}{i}\binom{i}{j}\binom{j}{k}$ is annihilated by the operators

$$\begin{gathered}(n+1)+(n+1)S_j+(n+1)S_iS_j-(n+1-k)S_iS_jS_n,\\ (k-n)+(k+1)S_k+(k+1)S_jS_k+(k+1)S_iS_jS_k.\end{gathered}$$

The coefficients of these operators are free of i and j, and they give rise to the annihilating operators

$$3(n+1)-(n+1-k)S_n \quad \text{and} \quad (k-n)+3(k+1)S_k$$

for the definite double sum $F(n,k) = \sum_i \sum_j f(n,k,i,j)$. Note that this sum has natural boundaries.

A certificate for the telescoper $P = 3(n+1) - (n+1-k)S_n$ is the pair

$$(Q_1, Q_2) = \big((n-k+1)S_n - 2(n+1),\ (n-k+1)S_jS_n - (n+1)S_j\big)$$

because $P - (S_i - 1)Q_1 - (S_j - 1)Q_2$ is equal to the first of the two annihilating operators for $f(n,k,i,j)$ stated above. □

Theorem 5.24 *Let $A = C[x_1,\dots,x_n,t_1,\dots,t_m][\partial_{x_1},\dots,\partial_{x_n},\partial_{t_1},\dots,\partial_{t_m}]$ be an Ore algebra such that for each ∂_{x_i} $(i=1,\dots,n)$ the polynomial $p = x_i$ meets the requirements of Lemma 5.19. Suppose further that $\sigma_{x_i}(x_i) \in C[x_i]$ for all i.*

Let $I \subseteq A$ be holonomic and let T be the set of all operators

$$P \in C[t_1,\dots,t_m][\partial_{t_1},\dots,\partial_{t_m}]$$

so that there exist $Q_1,\dots,Q_n \in A$ with $P - \partial_{x_1}Q_1 - \cdots - \partial_{x_n}Q_n \in I$. Then T is holonomic. □

Proof It is left as an exercise (Exercise 17) to show that T is an ideal of $C[t_1,\dots,t_m][\partial_{t_1},\dots,\partial_{t_m}]$. According to Definition 4.67, it then remains to show that for every subset $U \subseteq \{t_1,\dots,t_m,\partial_{t_1},\dots,\partial_{t_m}\}$ with $|U| = m+1$, we have $T \cap C[U] \neq \{0\}$.

Let $U \subseteq \{t_1, \dots, t_m, \partial_{t_1}, \dots, \partial_{t_m}\}$ be such that $|U| = m + 1$. Since I is holonomic, we have $I \cap C[U, \partial_{x_1}, \dots, \partial_{x_n}] \neq \{0\}$. Let L be a nonzero element of this elimination ideal and let $P \in C[U]$ and $Q_1, \dots, Q_n \in C[U, \partial_{x_1}, \dots, \partial_{x_n}]$ be such that $L = P - \partial_{x_1} Q_1 - \cdots - \partial_{x_n} Q_n$. Note that the requirement $P \in C[U]$ can be ensured using multivariate right-division with remainder (analogous to left-division with remainder outlined in Algorithm 4.76). By choosing a term order with $\partial_{x_1} < \partial_{x_2} < \cdots$, it can further be assumed that $Q_i \in C[U, \partial_{x_1}, \dots, \partial_{x_i}]$ for every i.

If P is nonzero, we are done. Otherwise, if P is zero, then Q_i must be nonzero for at least one i, because L is nonzero. Let i be minimal with $Q_i \neq 0$ and let $k \in \mathbb{N}$ be maximal such that $\partial_{x_i}^k$ is a right factor of $\partial_{x_i} Q_i$. By Lemma 5.19, we have $\sigma_{x_i}^{\overline{k}}(x_i) Q_i = \partial_{x_i} M - \tilde{L}$ for some $M \in C[U, \partial_{x_1}, \dots, \partial_{x_i}, x_i]$ and some nonzero $\tilde{L} \in C[U, \partial_{x_1}, \dots, \partial_{x_{i-1}}]$, and consequently

$$\sigma_{x_i}^{\overline{k}}(x_i) L = \tilde{L} - \partial_{x_i} \tilde{Q}_i - \sum_{j>i} \partial_{x_j} \sigma_{x_i}^{\overline{k}}(x_i) Q_j .$$

Now let $\tilde{P} \in C[U]$ and $\tilde{Q}_1, \dots, \tilde{Q}_{i-1} \in C[U, \partial_{x_1}, \dots, \partial_{x_{i-1}}]$ be such that $\tilde{L} = \tilde{P} - \partial_{x_1} \tilde{Q}_1 - \cdots - \partial_{x_{i-1}} \tilde{Q}_{i-1}$. If $\tilde{P}$ is nonzero, we are done. Otherwise, if $\tilde{P}$ is zero, repeat the argument from before. As the minimal i with $\tilde{Q}_i \neq 0$ is strictly smaller than the minimal i with $Q_i \neq 0$, the construction cannot be repeated infinitely often. Once it terminates, we have encountered a nonzero element of T. ∎

Translated into the language of summation and integration, Theorem 5.24 asserts that multiple definite sums and integrals over a multivariate holonomic function with natural boundaries are holonomic. Note that also the mixed case involving sums as well as integrals is covered by this statement.

In nontrivial examples, the annihilating operators of the summand/integrand whose coefficients do not involve the summation/integration variable(s) tend to be much larger than the telescopers extracted from them. If it is known that the sum/integral at hand has natural boundaries, it would be desirable to avoid the explicit computation of these large operators and to compute the telescopers more directly. In the notation of Theorem 5.24, the question is whether we can get generators of T from the given generators of I without explicitly constructing elements of the elimination ideal $E = I \cap C[t_1, \dots, t_m, \partial_{x_1}, \dots, \partial_{x_n}, \partial_{t_1}, \dots, \partial_{t_m}]$.

This can be done by reorganizing the computation as follows. Instead of first eliminating the summation/integration variables and then right-reducing with respect to $\partial_{x_1}, \dots, \partial_{x_n}$ in order to obtain the desired telescopers, we would like to first right-reduce with respect to $\partial_{x_1}, \dots, \partial_{x_n}$ and then eliminate the summation/integration variables. The problem with this idea is that right-reduction does not blend well with I being a left ideal. To make the idea work, we must overcome some of the non-commutativity. The elements $t_1, \dots, t_m, \partial_{t_1}, \dots, \partial_{t_m}$ are not problematic because they commute with $\partial_{x_1}, \dots, \partial_{x_n}$. Only the summation/integration variables $x_1, \dots, x_n$ are critical. We need to avoid multiplying by them from the left after doing right-reduction with respect to $\partial_{x_1}, \dots, \partial_{x_n}$.

The solution is to first augment the given basis of I with a number of left multiples of generators by terms in $x_1, \dots, x_n$, then to do the right-reduction by $\partial_{x_1}, \dots, \partial_{x_n}$, and finally to perform an elimination of $x_1, \dots, x_n$ using only multiplications by $t_1, \dots, t_m$ and $\partial_{t_1}, \dots, \partial_{t_m}$. We do not know in advance which left multiples of the generators of I need to be added to the basis in order to find a result, but we can be sure that the approach will work if we add sufficiently many.

Algorithm 5.25 *(Takayama)*
Input: *An ideal $I = \langle b_1, \dots, b_k \rangle$ of an Ore algebra*

$$A_{x,t} := C[x_1, \dots, x_n, t_1, \dots, t_m][\partial_{x_1}, \dots, \partial_{x_n}, \partial_{t_1}, \dots, \partial_{t_m}],$$

and a threshold $d \in \mathbb{N}$.
Output: *A subset of the ideal T consisting of all operators*

$$P \in A_t := C[t_1, \dots, t_m][\partial_{t_1}, \dots, \partial_{t_m}]$$

such that there exist $Q_1, \dots, Q_n \in A_{x,t}$ with $P - \sum_{i=1}^n \partial_{x_i} Q_i \in I$. If d is sufficiently large, the output will be a basis of T.

1 *Let B be the set of all τb_i with $i = 1, \dots, k$ and where τ runs through all terms $x_1^{e_1} \cdots x_n^{e_n}$ with $e_1 + \cdots + e_n \le d$.*
2 *Replace all elements in B by their right-remainders w.r.t. $\{\partial_{x_1}, \dots, \partial_{x_n}\}$.*
3 *Let $\tau_1 = 1$ and let $\tau_2, \dots, \tau_\ell \neq 1$ be monomials in $x_1, \dots, x_n$ such that each element of B can be viewed as an A_t-linear combination of $\tau_1, \dots, \tau_\ell$.*
4 *Replace each element $b \in B$ by the vector $([\tau_1]b, \dots, [\tau_\ell]b) \in A_t^\ell$.*
5 *Let M be the A_t-module generated by B and compute a basis E of the elimination module $M \cap \langle (1, 0, \dots, 0) \rangle$, for example using Gröbner bases with respect to a POT order.*
6 *Return the first coordinates of the elements of E.*

Theorem 5.26 *Algorithm 5.25 is correct and terminates.* □

Proof Termination is clear. Correctness consists of two points: 1. every element of the output is an element of T, and 2. for sufficiently large d, the output is a basis of T.

1. Let $P \in E$. It is clear that $P \in A_t$. We have to show that there are $Q_1, \dots, Q_n \in A_{x,t}$ with $P - \sum_{i=1}^n \partial_{x_i} Q_i \in I$. By definition of E, we have $(P, 0, \dots, 0) \in M$, i.e., $P + 0\tau_2 + \cdots + 0\tau_\ell$ is an A_t-linear combination of the elements of the set B computed in line 2. Therefore, there exist $Q_1, \dots, Q_n \in A_{x,t}$ such that $P - \sum_{i=1}^n \partial_{x_i} Q_i$ is an A_t-linear combination of the elements of the set B computed in line 1. But then it is also an $A_{x,t}$-linear combination of $b_1, \dots, b_k$ and thus an element of I. This shows that $P \in T$.
2. If E_d denotes the output of the algorithm for a specific choice d, then we have $\langle E_1 \rangle \subseteq \langle E_2 \rangle \subseteq \cdots$. By the ascending chain condition, there is a d such that

$\langle E_d \rangle = \langle E_{d+1} \rangle = \cdots$. We show that $\langle E_d \rangle = T$ for such a d. The inclusion "$\subseteq$" amounts to part 1 of the proof. For "$\supseteq$", let $P \in T$ and let $Q_1, \ldots, Q_n \in A_{x,t}$ be such that $P - \sum_{i=1}^n \partial_{x_i} Q_i \in I$. Being an element of I means to be an $A_{x,t}$-linear combination of $b_1, \ldots, b_k$. As the coefficients of such a linear combination involve only finitely many terms, there is an $m \in \mathbb{N}$ such that $P - \sum_{i=1}^n \partial_{x_i} Q_i$ is also an A_t-linear combination of the operators τb_i with $i = 1, \ldots, n$ and τ running through all terms $x_1^{e_1} \cdots x_n^{e_n}$ with $e_1 + \cdots + e_n \le m$. We have thus shown that P is an element of $\langle E_m \rangle$. By the choice of d, it must then also be an element of $\langle E_d \rangle$. ∎

Example 5.27 The ideal $I = \langle (n+1-k)^2 S_n - (n+1)^2, (k+1)^2 S_k + (k-n)^2 \rangle \subseteq C[n,k][S_n, S_k]$ consists of annihilating operators of $\binom{n}{k}^2$. We want to find a telescoper for I using Algorithm 5.25.

With $d = 0$, we set $B = \{(n+1-k)^2 S_n - (n+1)^2, (k+1)^2 S_k + (k-n)^2\}$ in line 1 and update the set to $B = \{(n+1-k)^2 S_n - (n+1)^2, 2nk - n^2\}$ in line 2, because $(k+1)^2 S_k - (k-n)^2 = (S_k - 1)k^2 + k^2 - (k-n)^2$. Taking $\tau_1 = 1, \tau_2 = k, \tau_3 = k^2$ in line 3, we get

$$B = \{\begin{pmatrix} (n+1)^2 S_n - (n+1)^2 \\ -2(n+1) S_n \\ S_n \end{pmatrix}, \begin{pmatrix} -n^2 \\ 2n \\ 0 \end{pmatrix}\}$$

in line 4, and it is easy to see by inspection that the elimination module $M \cap \langle (1,0,0) \rangle$ computed in line 5 is $\{0\}$.

Trying again with $d = 1$, we get

$$B = \{(n+1-k)^2 S_n - (n+1)^2,\ 2nk - n^2,\ k(n+1-k)^2 S_n - k(n+1)^2,\ -k^2 + 2k^2 n - kn^2\}$$

in line 2. We therefore take $\tau_1 = 1, \tau_2 = k, \tau_3 = k^2, \tau_4 = k^3$ in line 3 and get

$$B = \{\begin{pmatrix} (n+1)^2 S_n - (n+1)^2 \\ -2(n+1) S_n \\ S_n \\ 0 \end{pmatrix}, \begin{pmatrix} -n^2 \\ 2n \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ (n+1)^2 S_n - (n+1)^2 \\ -2(n+1) S_n \\ S_n \end{pmatrix}, \begin{pmatrix} 0 \\ -n^2 \\ 2n-1 \\ 0 \end{pmatrix}\}$$

in line 4. This time, the elimination module in line 5 is

$$M \cap \langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rangle = \langle \begin{pmatrix} (n+1)^3 S_n - 2(n+1)^2(2n+1) \\ 0 \\ 0 \\ 0 \end{pmatrix} \rangle,$$

so we have found the telescoper $(n+1)^3 S_n - 2(n+1)^2(2n+1)$. □

If we know that T is holonomic, then we can apply Algorithm 5.25 for $d = 0, 1, 2, \ldots$ until the output is a holonomic ideal. This should be implemented in a way that avoids obvious recomputations. Knowing a basis of the module M for $d-1$, the iteration for d needs to construct only the τ-multiples of $b_1, \ldots, b_n$ for terms $\tau = x_1^{e_1} \cdots x_n^{e_n}$ with $e_1 + \cdots + e_n = d$, and in line 5 update M to the module generated by the basis of the M from the previous iteration and the new vectors constructed in line 4. Since we even have a Gröbner basis for the old M, it may pay off to replace the new vectors with their normal form with respect to this Gröbner basis.

Note that even if the output is holonomic, it may still be smaller than T (cf. Exercise 11 in Sect. 4.5).

Exercises

1. Writing D_x^{-1} for the integral operator $\int_0^x dx$, do we necessarily have $D_x^{-1} D_x = \mathrm{id}$ or $D_x D_x^{-1} = \mathrm{id}$ or at least $D_x D_x^{-1} = D_x^{-1} D_x$?

2⋆. In 2023, some computer algebra system simplified the sum $\sum_{k=0}^{n} \frac{1}{(k-300)(k-301)}$ to $-\frac{1}{301} - \frac{1}{n-300}$. Discuss.

3. Show that a rational function $r = p/q \in C(n, k)$ is proper hypergeometric if and only if its denominator admits a factorization into integer-linear factors, i.e., into factors of the form $an + bk + c$ with $a, b \in \mathbb{Z}$ and $c \in C$.

4. Holonomy is a sufficient condition for the existence of a telescoper. Is it also necessary?

5. Show that the certificate of a telescoper is never unique.

6⋆. Prove or disprove:

a. $\Gamma(n/2 + k/3)$ is proper hypergeometric.
b. $n^{\underline{k}}$ is proper hypergeometric.
c. If h is proper hypergeometric and $h \neq 0$, then so is $1/h$.
d. If C is algebraically closed, then every univariate hypergeometric term is proper hypergeometric.

7⋆. Show that the degree bound for the numerator of $(L \cdot h)/h$ in the proof of Theorem 5.14 can be improved to

$$\deg_k(p) + r\Bigg(\sum_{m=1}^{M}(u_m + u'_m + v_m + b'_m) + \max\Big(0, \sum_{m=1}^{M}(a_m + b_m - u_m - v_m)\Big) + \max\Big(0, \sum_{m=1}^{M}(a'_m + v'_m - u'_m - b'_m)\Big)\Bigg).$$

8*. Generalize the argument in the proof of Theorem 5.14 to a more general ansatz of the form $L = \sum_{i=0}^{r}\sum_{j=0}^{s} \ell_{i,j} S_n^i S_k^j$. Show that r and s can be chosen in such a way that there is a telescoper of order $r \le \sum_{m=1}^{M}(a_m + b_m + u_m + v_m)$.

9. Show that **a.** $f(x) = \sum_{n=1}^{\infty}(x^2+n^2)^{-1}$ and **b.** $a_n := \int_0^1 (x+n)^{-1}dx$ are not D-finite, although $(x^2+n^2)^{-1}$ and $(x+n)^{-1}$ are.

Hint: Recall that $\coth(x) = \frac{1}{x} + \sum_{n=1}^{\infty} \frac{2x}{n^2\pi^2+x^2}$.

10. Simplify the following definite sums:

a. $\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}^3$ (Dixon) **b.** $\sum_{k=0}^{n}(-2)^k\binom{2n}{k}\binom{4n-k}{2n}$

c. $\sum_{k=0}^{n} 4^n(-4)^{-k}\binom{2n-k}{k}$ **d.** $\sum_{k=0}^{n} \frac{(-1)^k}{k+1}\binom{n+k}{2k}\binom{2k}{k}$ $(n \ge 1)$

e. $\sum_{k=0}^{n}\binom{n}{2k}\binom{2k}{k}4^{-k}$ **f.** $\sum_{k=0}^{n}\binom{n}{k}^2/\binom{n+k}{k}^2$ $(n \ge 1)$

g. $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{n+k}{k}$ **h.** $\sum_{k=0}^{n}(-1)^n\binom{n}{k}\frac{(n-1)!}{(k-1)!}x^{\underline{k}}$

i. $\sum_{k=0}^{n}\frac{(-4)^k}{2k+1}\binom{n+k}{2k}$ **j.** $\sum_{k=0}^{n}\binom{n}{k}^2/\binom{2n}{2k}$ $(n \ge 1)$

k. $\sum_{k=0}^{\infty}\binom{n+k}{k}2^{-k}$ **l.** $\sum_{k=0}^{n} 2^{-n-2k}\binom{n}{k}\binom{n-k}{k}$

11. Simplify the following definite integrals:

a. $\int_0^\infty \frac{\sin(tx)^2}{x^2}dx$ $(t > 0)$

b. $\int_0^\infty \frac{1}{\sqrt{x^3+t}}dx$ $(t > 0)$; use $\int_0^\infty \frac{1}{\sqrt{x^3+1}}dx = \frac{2\Gamma(1/3)\Gamma(7/6)}{\sqrt{\pi}}$.

c. $\int_{-1}^{1} P_n(x)^2dx$, where $P_n(x)$ is the nth Legendre polynomial.

d. $\int_{-\infty}^{\infty} e^{xt}\operatorname{Ai}(x)dx$, where $\operatorname{Ai}(x)$ is the first Airy function; use $\int_{-\infty}^{\infty}\operatorname{Ai}(x)dx = 1$.

e. $\int_0^\infty e^{-ax}\operatorname{erf}(\sqrt{bx})dx$, where $\operatorname{erf}(x)$ is the error function.

f. $\int_0^\infty J_n(tx)dx$ $(t > 0)$, where $J_n(x)$ is the nth Bessel function of the first kind.

12. Find a definite single sum $F(n) = \sum_k f(n,k)$ over a proper hypergeometric term $f(n,k)$ with natural boundaries such that $F(n)$ is not hypergeometric.

13.** Show that the following integrals are D-finite with respect to their free variable(s).

a. $W_n := \int_0^{\pi/2}\sin(x)^n dx$ (Wallis' integral)

b. $K(t) := \int_0^{\pi/2}\frac{1}{\sqrt{1-t^2\sin(x)^2}}dx$ (Complete elliptic integral of the first kind)

c. $J_n(t) := \int_0^{\pi}\cos(nx - t\sin(x))dx$ (Bessel function of the first kind)

Hint: Start by finding substitutions that make the integrands D-finite.

14. (Volker Strehl) Prove the following identity:

$$\sum_{j,k}\binom{n}{k}\binom{n+k}{k}\binom{k}{j}^3 = \sum_k\binom{n}{k}^2\binom{n+k}{k}^2$$

for $n \in \mathbb{N}$.

15. Suppose that f is a bivariate holonomic function, say in the differential case. Show that setting one of the variables to zero gives a univariate holonomic function.

Hint: Consider a telescoping relation in which the roles of x and D_x are exchanged.

16****.** For the hypergeometric term $h = \frac{\Gamma(3n+4k)\Gamma(4n+3k)\Gamma(2n-k)\Gamma(2n-2k)}{\Gamma(2n+3k)\Gamma(3n+k)\Gamma(3n-k)\Gamma(3n-2k)}$, which terms $S_n^i S_k^j$ can be added to the ansatz $L = \sum_{i=0}^{6} \sum_{j=0}^{6} \ell_{i,j} S_n^i S_k^j$ such that the degrees of numerator and denominator of $(L \cdot h)/h$ do not increase?

17. Let $R_{x,t}$ be a ring and R_t be a subring of $R_{x,t}$. Let

$$A_{x,t} = R_{x,t}[\partial_{x_1}, \dots, \partial_{x_n}, \partial_{t_1}, \dots, \partial_{t_m}]$$

be an Ore algebra such that $A_t = R_t[\partial_{t_1}, \dots, \partial_{t_m}]$ is a subalgebra of $A_{x,t}$. Let I be an ideal of $A_{x,t}$ and let T be the set of all operators $P \in A_t$ such that there exist $Q_1, \dots, Q_n \in A$ with $P - \sum_{i=1}^{n} \partial_{x_i} Q_i \in I$. Show that T is an ideal of A_t.

18***.** Let f_1, f_2 be D-finite functions with respect to the action of an Ore algebra $C(x,t)[\partial_x, \partial_t]$, and let $P_1, P_2 \in C(t)[\partial_t]$ be telescopers for f_1, f_2, respectively. Suppose there exist $L_1, L_2 \in C(x,t)[\partial_x]$ as well as $L_1, L_2 \in C(x,t)[\partial_t]$ with $L_1 \cdot f_1 = L_2 \cdot f_2 = 0$ and $\operatorname{gcrd}(L_1, L_2) = 1$. Prove or disprove:

a. $P_1 \oplus P_2$ is a telescoper for $f_1 + f_2$.

b. $P_1 \otimes P_2$ is a telescoper for $f_1 f_2$.

19***.** Let $f(x,t)$ be a holonomic function and let P be a telescoper (w.r.t. x) of $f(x,t)$. Let $h(t)$ be a univariate hypergeometric or hyperexponential term. Construct a telescoper (w.r.t. x) of $h(t) f(x,t)$.

20***.** Show that Lemma 5.19 is not needed for definite sums over proper hypergeometric terms that can be written in the form $r(n,k)h(n)$, where $r(n,k)$ is a rational function and $h(n)$ is a hypergeometric term which is constant with respect to k. More precisely, show that every such term has an annihilating operator $L \in C[n][S_n, S_k]$ which can be written as $L = P - (S_k - 1)Q$ for some nonzero $P \in C[n][S_n]$ and some $Q \in C[n][S_n, S_k]$.

References

Some of the ideas presented in this section predate the age of computer algebra. The technique to use linear algebra for finding a recurrence that does not involve the summation variable of a proper hypergeometric term was introduced in the 1940s by Fasenmyer [187, 188]. The technique is known as Sister Celine's method, referring to Fasenmyer's clerical name, and it is covered in several textbooks [284, 356, 364]. Sister Celine's method was introduced into computer algebra by Verbaeten in 1974 [450], who proved that the method always succeeds and proposed optimizations. This work did not receive much attention until Zeilberger entered the stage in the early 1990s. Sister Celine's method was one of the motivations that led to his seminal paper on special function identities [468]. His article in turn motivated a lot of subsequent development, some of which is covered in the next sections.

Wegschaider implemented a variant of Sister Celine's algorithm for nested sums in Mathematica for his master's thesis in 1997 [453]. His thesis contains Lemma 5.19 as Theorem 3.2. Gröbner bases computations for ideals in Ore algebras were first used for proving identities by Chyzak and Salvy [157]. Takayama's algorithm appeared in [423, 424]. An algorithm for solving the contraction problem was proposed by Tsai [427]. For the univariate case, which is much easier, see [428, 474].

The Wilf-Zeilberger conjecture posed in [458] states that the converse of Theorem 5.14 is also true: a hypergeometric term is holonomic if and only if it is proper. Depending on what exactly is understood as a hypergeometric term, the conjecture is either true (as shown by Payne [352], Abramov and Petkovšek [16], and Chen and Koutschan [130]) or false (as pointed out by Payne [352] and Abramov and Petkovšek [18]). The paper [18] of Abramov and Petkovšek also contains an elementary proof of the so-called Ore-Sato theorem [343, 380], which roughly says that every multivariate hypergeometric term can be written as an expression like in Definition 5.13, except that p may in general be a rational function rather than a polynomial.

A very different approach to definite integration was explored by Regensburger, Rosenkranz and collaborators, who considered enriched operator algebras where in addition to a derivation operator D_x one also has integration operators as well as operators for evaluation [228, 365, 373, 374].

5.3 Further Closure Properties

The concept of telescopers was motivated in the previous section for finding annihilating operators of definite sums and integrals. The concept is more powerful than that and applies as well to a number of further operations. For example, consider what happens if we exchange the roles of x and D_x. If a bivariate function f depending on two continuous variables x and y has an annihilating operator which can be written in the form $P - xQ$ with $P \in C[y][D_y]$ nonzero and $Q \in C[x, y][D_x, D_y]$, then setting x to zero in the relation $(P - xQ) \cdot f = 0$ shows that the univariate function $y \mapsto f(0, y)$ is annihilated by P. This idea extends directly to more variables, to evaluation points other than zero, to the discrete case, and even to functions involving discrete as well as continuous variables.

Theorem 5.28 *Let F be a $C[x, t_1, \dots, t_m][\partial_x, \partial_{t_1}, \dots, \partial_{t_m}]$-module where ∂_x is either D_x or S_x, let F_0 be a $C[t_1, \dots, t_m][\partial_{t_1}, \dots, \partial_{t_m}]$-module, and let $\phi\colon F \to F_0$ be a $C[t_1, \dots, t_m][\partial_{t_1}, \dots, \partial_{t_m}]$-module homomorphism with $\phi(x \cdot f) = 0$ for all $f \in F$. Then ϕ maps holonomic elements of F to holonomic elements of F_0.* □

Proof For $A = C[x, t_1, \dots, t_m][D_x, \partial_{t_1}, \dots, \partial_{t_m}]$ consider the Ore algebra

$$\tilde{A} := C[\tilde{x}, t_1, \ldots, t_m][\partial_{\tilde{x}}, \partial_{t_1}, \ldots, \partial_{t_m}].$$

with $\partial_{\tilde{x}}\tilde{x} = \tilde{x}\partial_{\tilde{x}} - 1$. Note that A and $\tilde{A}$ are isomorphic as we can identify $x \in A$ with $\partial_{\tilde{x}} \in \tilde{A}$ and $D_x \in A$ with $\tilde{x} \in \tilde{A}$, and the elements of C as well as the t_j and the ∂_{t_j} with themselves. If $f \in F$ is holonomic with respect to the action of A, it is also holonomic with respect to the action of $\tilde{A}$. Let $\tilde{I} \subseteq \tilde{A}$ be a holonomic ideal of annihilating operators of f. We have $\sigma_{\tilde{x}}(\tilde{x}) = \tilde{x} \in C[\tilde{x}]$, and the polynomial $p = \tilde{x}$ meets the requirements of Lemma 5.19 (Exercise 4). We can thus apply Theorem 5.24 and conclude that there exists a holonomic ideal $T \subseteq C[t_1, \ldots, t_m][\partial_{t_1}, \ldots, \partial_{t_m}]$ of telescopers with respect to $\tilde{A}$. To be a telescoper with respect to $\tilde{A}$ means that for every $L \in T$ there exist $Q \in A$ such that $L - xQ \in I$. Then $(L - xQ) \cdot f = 0$ implies $\phi(L \cdot f) = 0$, so L is an annihilating operator of $\phi(f)$.

For $A = C[x, t_1, \ldots, t_m][S_x, \partial_{t_1}, \ldots, \partial_{t_m}]$, the argument is the same, except that for $\tilde{A}$ we now take the commutation rule $\partial_{\tilde{x}}\tilde{x} = \tilde{x}\partial_{\tilde{x}} - (\tilde{x} + 1)$ so that $\tilde{x} \in \tilde{A}$ plays the role of $\Delta_x = S_x - 1 \in A$ and $\partial_{\tilde{x}} \in \tilde{A}$ plays the role of $x \in A$. ■

Example 5.29

1. Suppose that C is a subfield of $\mathbb{C}$, and let U be an open subset of $\mathbb{C}^{n+m}$. Let $\xi \in C^n$ and let U_ξ be an open subset of $\mathbb{C}^m$ such that $\{\xi\} \times U_\xi \subseteq U$. If $f : U \to \mathbb{C}$ is holonomic with respect to

$$C[x_1, \ldots, x_n, t_1, \ldots, t_m][D_{x_1}, \ldots, D_{x_n}, D_{t_1}, \ldots, D_{t_m}],$$

the function $f_\xi : U_\xi \to \mathbb{C}$ defined by $f_\xi(t_1, \ldots, t_m) = f(\xi, t_1, \ldots, t_m)$ is holonomic with respect to $C[t_1, \ldots, t_m][D_{t_1}, \ldots, D_{t_m}]$. After a change of variables that moves ξ to zero, this follows directly from an n-fold application of Theorem 5.28.
2. Let $\xi \in \mathbb{Z}^n$. If $f : \mathbb{Z}^{n+m} \to C$ is holonomic with respect to

$$C[x_1, \ldots, x_n, t_1, \ldots, t_m][S_{x_1}, \ldots, S_{x_n}, S_{t_1}, \ldots, S_{t_m}],$$

the function $f_\xi : \mathbb{Z}^n \to C$ defined by $f_\xi(t_1, \ldots, t_m) = f(\xi, t_1, \ldots, t_m)$ is holonomic with respect to $C[t_1, \ldots, t_m][S_{t_1}, \ldots, S_{t_m}]$. Again, this follows from an n-fold application of Theorem 5.28 and a change of variables moving ξ to zero. □

A consequence of Theorem 5.28 is that we can drop the restriction to definite integrals with natural boundaries made in the previous section. More precisely, consider a definite integral $F(t) = \int_a^b f(x,t)dx$ for some holonomic function f defined on a certain subset of $\mathbb{C}$, and for two constants $a, b \in C \subseteq \mathbb{C}$ in the domain of f. We know from the previous section that there exist $P \in C[t][D_t] \setminus \{0\}$ and $Q \in C[x,t][D_x, D_t]$ such that $(P - D_x Q) \cdot f = 0$, which means that for

$g := Q \cdot f$ we have $P \cdot f = D_x \cdot g$. This gives $P \cdot F = g|_{x=b} - g|_{x=a}$. By Theorem 5.28, $g|_{x=b}$ and $g|_{x=a}$ are holonomic functions in t. If $L \in C[t][D_t]$ is a common left multiple of an annihilating operator for $g|_{x=b}$ and an annihilating operator for $g|_{x=a}$, it will annihilate the right hand side, so we will have $LP \cdot F = 0$, proving that F is holonomic. This reasoning extends to integrals $F(t_1, \ldots, t_m) = \int_a^b f(x, t_1, \ldots, t_m)dx$ involving several parameters.

As another application of Theorem 5.28, we can now close a gap that we left open when we discussed D-finite closure properties related to composition (Theorem 4.72). As the argument uses the equivalence of D-finiteness and holonomy, it only works in the differential case. The corresponding statement for the shift case will be settled later in a different way.

Theorem 5.30 *(See Theorem 5.36 for the shift case) Let $f \in C[[x_1, \ldots, x_n]]$ be D-finite (w.r.t. $C[x_1, \ldots, x_n][D_{x_1}, \ldots, D_{x_n}]$) and let $g_1, \ldots, g_n \in C[[z_1, \ldots, z_m]]$ be algebraic over $C(z_1, \ldots, z_m)$. If the composition $f(g_1, \ldots, g_n)$ is a well-defined element of $C[[z_1, \ldots, z_m]]$, then it is D-finite (w.r.t. $C[z_1, \ldots, z_m][D_{z_1}, \ldots, D_{z_m}]$).* □

Proof The main difference to Theorem 4.72 is that $g_1, \ldots, g_n$ are no longer assumed to be algebraically independent. Some of the g_i may even be identical to zero. Let us assume without loss of generality that the variables are indexed in such a way that $g_1, \ldots, g_k$ are nonzero and $g_{k+1} = \cdots = g_n = 0$. By Theorem 5.28, $\tilde{f} := f(x_1, \ldots, x_k, 0, \ldots, 0)$ is holonomic, and it remains to argue that $\tilde{f}(g_1, \ldots, g_k)$ is holonomic. Using new variables $z_{m+1}, \ldots, z_{m+k}$, we reduce the situation to the case of Theorem 4.72. The algebraic series $z_{m+1}g_1, \ldots, z_{m+k}g_k$ are algebraically independent over C, so by Theorem 4.72, the series $\tilde{f}(z_{m+1}g_1, \ldots, z_{m+k}g_k) \in C[[z_1, \ldots, z_m, z_{m+1}, \ldots, z_{m+k}]]$ is holonomic. By Theorem 5.28, setting $z_{m+1} = \cdots = z_{m+k} = 1$ preserves holonomy, so $f(g_1, \ldots, g_n) = \tilde{f}(g_1, \ldots, g_k)$ is holonomic. ■

Theorem 5.30 allows us to consider definite integrals with more sophisticated integration ranges. For example, the result of integrating two variables of a trivariate D-finite function over a disk is D-finite. More generally, the integration range can be any *semialgebraic* set. A subset S of $\mathbb{R}^n$ is called semialgebraic if there is a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $(\xi_1, \ldots, \xi_n) \in S \iff p(\xi_1, \ldots, \xi_n) = 0$, or such that $(\xi_1, \ldots, \xi_n) \in S \iff p(\xi_1, \ldots, \xi_n) \geq 0$, or if S is the union or the intersection of finitely many semialgebraic sets. Integrals over such sets naturally translate into iterated univariate integrals whose boundaries are algebraic functions. Even more generally, we can allow the integration range to vary with the free parameter(s) of the integral, by considering families $S(t_1, \ldots, t_m)$ of subsets of $\mathbb{R}^n$ defined through polynomials $p \in \mathbb{Q}[x_1, \ldots, x_n, t_1, \ldots, t_m]$ via $(\xi_1, \ldots, \xi_n) \in S(\tau_1, \ldots, \tau_m) \iff p(\xi_1, \ldots, \xi_n, \tau_1, \ldots, \tau_m) = 0$, or such that $(\xi_1, \ldots, \xi_n) \in S(\tau_1, \ldots, \tau_m) \iff p(\xi_1, \ldots, \xi_n, \tau_1, \ldots, \tau_m) \geq 0$, or finite unions or intersections of such sets. Integrals of D-finite functions in $x_1, \ldots, x_n, t_1, \ldots, t_m$ over such sets are D-finite functions in $t_1, \ldots, t_m$.

Real numbers which can be expressed as an integral over a semialgebraic set of a rational function with coefficients in $\mathbb{Q}$ are called *periods*. The periods form a countable subring of $\mathbb{R}$ which contains many numbers appearing in number theory, including real algebraic numbers, π, $\log(2)$, $\zeta(3)$, $\Gamma(\frac{1}{4})$, and Catalan's constant $G = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2}$. It is not known whether e or $1/\pi$ are periods, and in fact, it is only known for some artificially constructed numbers that they are not periods. It is also not known whether there is an algorithm for deciding whether two periods, given in terms of an integral, are equal. This can be troublesome if we want to apply D-finite technology to prove a relation among two multidimensional definite integrals involving a free parameter, and we indeed succeed to derive a common annihilating operator for both sides of the conjectured identity, but then fail to complete the job because checking initial values requires the comparison of some complicated constants.

For definite sums with finite summation ranges, the evaluation of initial values is less problematic. It just requires adding some finitely many numbers. Infinite summation ranges are sometimes more problematic because we may end up having to compare constants that are defined by infinite series. An infinite sum that works smoothly arises in the multivariate analog of Theorem 2.33, which says that the generating function of a D-finite sequence is D-finite. Consider for simplicity a bivariate sequence $a\colon \mathbb{N}^2 \to C$ given by a holonomic ideal of annihilating operators in $C[k,n][S_k, S_n]$, and suppose we want to compute a holonomic ideal of annihilating operators in $C[x,n][D_x, S_n]$ of its generating function $f = \sum_{k=0}^{\infty} a_{k,n} x^k$ with respect to the first variable. Viewing this task as a definite summation problem, we first seek $P \in C[x,n][D_x, S_n] \setminus \{0\}$ and $Q \in C[k,x,n][S_k, D_x, S_n]$ such that $(P - \Delta_k Q) \cdot a_{k,n} x^k = 0$. For such P and Q we have $P \cdot f = -(Q \cdot a_{k,n} x^k)|_{k=0}$. Note that we have $\sum_{k=0}^{\infty} (g(k+1) - g(k)) = -g(0)$ for every function g, so the upper end of the summation range does not contribute to the inhomogeneous part. By Exercise 5, the annihilating ideal of $a_{k,n} x^k$ is holonomic w.r.t. $C[k,x,n][S_k, D_x, S_n]$, so by Theorem 5.24, the ideal of telescopers P is holonomic. This means that for every set $U \subseteq \{x, n, D_x, S_n\}$ with $|U| = 3$ there is a telescoper P only involving variables from U. But as the sum $\sum_{k=0}^{\infty} a_{k,n} x^k$ does not have natural boundaries, we are not done yet. In a second step, we apply Theorem 5.28 to see that $-(Q \cdot a_{k,n} x^k)|_{k=0}$ has a holonomic ideal of annihilating operators in $C[x,n][D_x, S_n]$, whenever Q is a certificate of a telescoper P. Since the ideal of annihilating operators of $-(Q \cdot a_{k,n} x^k)|_{k=0}$ is holonomic, it contains a certain operator $L \neq 0$ only containing variables from U. Then LP is a nonzero annihilating operator of the generating function, and since this construction works for every choice U of three variables, we obtain a holonomic ideal of annihilating operators for the generating function f.

The mere fact that the generating function of a holonomic sequence is a holonomic power series has already appeared in Exercise 5 of Sect. 4.5. The argument sketched above not only provides an independent argument for this, but also a reasonable approach to compute a holonomic ideal of annihilating operators for the generating function from a given holonomic ideal of the coefficient sequence.

Telescopers are also useful for going in the opposite direction. Again, in the interest of light notation, we only discuss a special case. Let a bivariate power series $a \in C[[x, y]]$ be given by a holonomic ideal of annihilating operators in $C[x, y][D_x, D_y]$, and suppose we want to compute a holonomic ideal of annihilating operators in $C[n, y][S_n, D_y]$ of its coefficient sequence $[x^n]a$ with respect to x. The idea is to write $[x^n]a = [x^{-1}]ax^{-n-1}$ and to exploit the fact that the derivative of a series cannot contain a term with exponent -1, which is an immediate consequence of the differentiation rule $(x^m)' = mx^{m-1}$. If $P \in C[n, y][S_n, D_y] \setminus \{0\}$ and $Q \in C[n, x, y][S_n, D_x, D_y]$ are such that $(P - D_x Q) \cdot ax^{-n-1} = 0$, then $P \cdot [x^n]a = [x^{-1}]D_x(Q \cdot ax^{-n-1})$, and no matter what Q is, the derivative of $Q \cdot ax^{-n-1}$ with respect to x cannot contain x^{-1}, so the right hand side is zero and the telescoper P for ax^{-n-1} is automatically an annihilating operator of $[x^n]a$.

The coefficient of x^{-1} of a series a is also called the *residue* of a (w.r.t. x) and denoted by $\operatorname{Res} a$ or $\operatorname{Res}_x a$. The fact that telescopers annihilate residues has further applications. First of all, it generalizes Theorem 5.28, because evaluating a function f at zero is the same as extracting the coefficient of x^0 from its series expansion, and this is the same as extracting the coefficient of x^{-1} from xf. But coefficient extraction is more powerful than evaluation because it can also be meaningful if f has a singularity at zero. For example, it makes perfect sense to ask for the coefficient of x^0 in $(x^2 - x + x^{-1})^n$, as a sequence in n.

The residue operator is only interesting for series that may involve terms with negative exponents. As long as we do not need to multiply such series, there is no problem in allowing series involving arbitrary integers as exponents. Indeed, if we define $C_{\mathbb{Z}}[[x_1, \dots, x_n]]$ as the set of all series $\sum_{k_1,\dots,k_n \in \mathbb{Z}} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ with $a_{k_1,\dots,k_n} \in C$ for all $k_1, \dots, k_n \in \mathbb{Z}$, then $C_{\mathbb{Z}}[[x_1, \dots, x_n]]$ is a perfectly well-defined $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$-module: we can add any two such series, multiply them by polynomials, and differentiate them. The residue of an element a of $C_{\mathbb{Z}}[[x_1, \dots, x_n]]$ is defined as $\operatorname{Res}_{x_1,\dots,x_n} a := [x_1^{-1} \cdots x_n^{-1}]a$. More generally, the residue of an element

$$\sum_{\substack{k_1,\dots,k_n \in \mathbb{Z} \\ u_1,\dots,u_m \in \mathbb{Z}}} a_{k_1,\dots,k_n,u_1,\dots,u_m} x_1^{k_1} \cdots x_n^{k_n} y_1^{u_1} \cdots y_m^{u_m}$$

of $C_{\mathbb{Z}}[[x_1, \dots, x_n, y_1, \dots, y_m]]$ with respect to $x_1, \dots, x_n$ is defined as

$$\operatorname{Res}_{x_1,\dots,x_n} a := \sum_{u_1,\dots,u_m \in \mathbb{Z}} a_{-1,\dots,-1,u_1,\dots,u_m} y_1^{u_1} \cdots y_m^{u_m}.$$

Theorem 5.31 *If $a \in C_{\mathbb{Z}}[[x_1, \dots, x_n, t_1, \dots, t_m]]$ is holonomic w.r.t.*

$$C[x_1, \dots, x_n, t_1, \dots, t_m][D_{x_1}, \dots, D_{x_n}, D_{t_1}, \dots, D_{t_m}],$$

then $\mathrm{Res}_{x_1,\dots,x_n} a \in C_{\mathbb{Z}}[[t_1,\dots,t_m]]$ *is holonomic w.r.t.*

$$C[t_1,\dots,t_m][D_{t_1},\dots,D_{t_m}].$$

□

Proof If $P \in C[t_1,\dots,t_m][D_{t_1},\dots,D_{t_m}] \setminus \{0\}$ and

$$Q_1,\dots,Q_n \in C[x_1,\dots,x_n,t_1,\dots,t_m][D_{x_1},\dots,D_{x_n},D_{t_1},\dots,D_{t_m}]$$

are such that $(P - D_{x_1}Q_1 - \cdots - D_{x_n}Q_n)\cdot a = 0$, then $P \cdot \mathrm{Res}_{x_1,\dots,x_n} a = \mathrm{Res}_{x_1,\dots,x_n}(D_{x_1}Q_1 \cdot a + \cdots + D_{x_n}Q_n \cdot a)$. The right hand side is zero, because for any i, the series $D_{x_i}Q_i \cdot a$ cannot contain terms in which the exponent of x_i is -1, therefore $\mathrm{Res}_{x_1,\dots,x_n} D_{x_i}Q_i \cdot a = 0$ for all i. It follows that every telescoper P for a is an annihilating operator for $\mathrm{Res}_{x_1,\dots,x_n} a$. The claim now follows from Theorem 5.24. ■

If we want to multiply or even divide series, it is necessary to restrict their support. Recall from Sect. 1.1 that in the univariate case, we can obtain the field $C((x))$ of formal Laurent series from the ring $C[[x]]$ via $C((x)) = \bigcup_{e\in\mathbb{Z}} x^e C[[x]]$. The analogous construction with more variables does not quite work. We could still define $C((x_1,\dots,x_n)) = \bigcup_{e_1,\dots,e_n\in\mathbb{Z}} x_1^{e_1}\cdots x_n^{e_n} C[[x_1,\dots,x_n]]$, and this is a ring. But then $C((x_1,\dots,x_n))$ is not a field (Exercise 6). If we want to have a field, we need to include series with larger supports. This can be done as follows; see [36] for more details on this construction.

- A *cone* is a subset Ξ of $\mathbb{R}^n$ which is closed under multiplication by nonnegative numbers. A cone Ξ is called *line-free* $x + y = 0 \Rightarrow x = y = 0$ for all $x, y \in \Xi$. For any vectors $b_1,\dots,b_\ell \in \mathbb{R}^n$, the cone generated by them is the set of all linear combinations $\beta_1 b_1 + \cdots + \beta_\ell b_\ell$ with $\beta_1,\dots,\beta_\ell \geq 0$. A cone is called *polyhedral* if it is generated by finitely many vectors with integer coefficients.
- For a line-free polyhedral cone $\Xi \subseteq \mathbb{R}^n$, we define $C_\Xi[[x_1,\dots,x_n]]$ as the subset of $C_{\mathbb{Z}}[[x_1,\dots,x_n]]$ consisting of all series $\sum_{k_1,\dots,k_n\in\mathbb{Z}} a_{k_1,\dots,k_n} x_1^{k_1}\cdots x_n^{k_n}$ with the property $(k_1,\dots,k_n) \notin \Xi \Rightarrow a_{k_1,\dots,k_n} = 0$. In other words, $C_\Xi[[x_1,\dots,x_n]]$ consists of all series whose support is contained in Ξ. For example, if Ξ is the cone generated by the unit vectors, then $C_\Xi[[x_1,\dots,x_n]]$ is the classical power series ring $C[[x_1,\dots,x_n]]$.
- For every line-free polyhedral cone $\Xi \subseteq \mathbb{R}^n$, the set $C_\Xi[[x_1,\dots,x_n]]$ together with the natural additional and multiplication forms a ring. The restriction of the support to Ξ ensures that the product is well-defined, because it implies that every coefficient of the product depends only on finitely many coefficients of the factors. Another property that generalizes from the classical power series ring is that an element a of $C_\Xi[[x_1,\dots,x_n]]$ admits a multiplicative inverse if and only if the coefficient of $x_1^0\cdots x_n^0$ in a is nonzero.
- Fix an additive order $\leq$ on $\mathbb{Z}^n$, i.e., a total order with $u \leq v \Rightarrow u + w \leq v + w$ for all $u, v, w \in \mathbb{Z}^n$, and let us say that a line-free polyhedral cone Ξ is

compatible with $\leq$ if $\Xi \cap \mathbb{Z}^n$ has a minimum with respect to $\leq$. We then define $C_{\leq}[[x_1, \dots, x_n]]$ as the union of all the rings $C_{\Xi}[[x_1, \dots, x_n]]$ where Ξ runs through all line-free polyhedral cones that are compatible with $\leq$. For any two line-free cones Ξ_1, Ξ_2 that are compatible with $\leq$ there is another line-free cone Ξ_3 that is compatible with $\leq$ such that $\Xi_1 \subseteq \Xi_3$ and $\Xi_2 \subseteq \Xi_3$. This implies that $C_{\leq}[[x_1, \dots, x_n]]$ is a ring.

- Now we are in a position from where we can continue like in the univariate case. For any fixed additive order $\leq$ on $\mathbb{Z}^n$, we define

$$C_{\leq}((x_1, \dots, x_n)) = \bigcup_{e_1,\dots,e_n \in \mathbb{Z}} x_1^{e_1} \cdots x_n^{e_n} C_{\leq}[[x_1, \dots, x_n]].$$

It can be checked that this is a field. It is called the field of *formal Laurent series* in $x_1, \dots, x_n$ over C with respect to the order $\leq$.

The field $C_{\leq}((x_1, \dots, x_n))$ contains not only the polynomial ring $C[x_1, \dots, x_n]$ but also a copy of the rational function field $C(x_1, \dots, x_n)$, because each rational function p/q can be identified with the series pq^{-1} in $C_{\leq}((x_1, \dots, x_n))$. Therefore, we can regard $C_{\leq}((x_1, \dots, x_n))$ not only as a $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$-module but also as a $C(x_1, \dots, x_n)[D_{x_1}, \dots, D_{x_n}]$-module. In this setting, we can also say that residues of a D-finite series are D-finite. By convention, we say that an element of $C_{\mathbb{Z}}[[x_1, \dots, x_n]]$ is D-finite if it belongs to $C_{\leq}((x_1, \dots, x_n))$ for a suitably chosen order $\leq$ and is D-finite as element of this field.

Several operations that can be performed on multivariate series can be reduced to residue operations and therefore preserve D-finiteness.

Definition 5.32 Let

$$a = \sum_{\substack{k_1,\dots,k_n \in \mathbb{Z} \\ u_1,\dots,u_m \in \mathbb{Z}}} a_{k_1,\dots,k_n,u_1,\dots,u_m} x_1 k_1 \cdots x_n k_n y_1 u_1 \cdots y_m u_m$$

be an element of $C_{\mathbb{Z}}[[x_1, \dots, x_n, y_1, \dots, y_m]]$.

1. The *diagonal*of a w.r.t. $x_1, \dots, x_n$ is defined as

$$\operatorname{diag}_{x_1,\dots,x_n} a := \sum_{k \in \mathbb{Z}} \sum_{u_1,\dots,u_m \in \mathbb{Z}} a_{k,k,\dots,k,u_1,\dots,u_m} x_n^k y_1^{u_1} \cdots y_m^{u_m}.$$

2. The *positive part*of a w.r.t. $x_1, \dots, x_n$ is defined as

$$[x_1^{>} \cdots x_n^{>}]a := \sum_{k_1,\dots,k_n \geq 1} \sum_{u_1,\dots,u_m \in \mathbb{Z}} a_{k_1,\dots,k_n,u_1,\dots,u_m} x_1^{k_1} \cdots x_n^{k_n} y_1^{u_1} \cdots y_m^{u_m}.$$

The nonnegative part, the negative part, and the nonpositive part of a are defined analogously.

3. Let

$$b = \sum_{\substack{k_1,\dots,k_n\in\mathbb{Z}\\ v_1,\dots,v_\ell\in\mathbb{Z}}} b_{k_1,\dots,k_n,v_1,\dots,v_\ell} x_1^{k_1}\cdots x_n^{k_n} z_1^{v_1}\cdots z_\ell^{v_\ell}$$

be an element of $C_{\mathbb{Z}}[[x_1,\dots,x_n,z_1,\dots,z_\ell]]$. The *Hadamard product* of a and b w.r.t. $x_1,\dots,x_n$ is the element

$$\sum_{\substack{k_1,\dots,k_n\in\mathbb{Z}\\ u_1,\dots,u_m\in\mathbb{Z}\\ v_1,\dots,v_\ell\in\mathbb{Z}}} a_{k_1,\dots,k_n,u_1,\dots,u_m} b_{k_1,\dots,k_n,v_1,\dots,v_\ell} x_1^{k_1}\cdots x_n^{k_n} y_1^{u_1}\cdots y_m^{u_m} z_1^{v_1}\cdots z_\ell^{v_\ell}$$

of $C_{\mathbb{Z}}[[x_1,\dots,x_n,y_1,\dots,y_m,z_1,\dots,z_\ell]]$, and denoted by $a\odot b$ or $a\odot_{x_1,\dots,x_n} b$. □

In the definition of the Hadamard product, we do not need to assume that the variable sets $\{y_1,\dots,y_m\}$ and $\{z_1,\dots,z_\ell\}$ are disjoint. However, the variable set $\{y_1,\dots,y_m,z_1,\dots,z_\ell\}$ should not overlap with the variable set $\{x_1,\dots,x_n\}$.

Theorem 5.33

1. *Diagonals of D-finite series are D-finite.*
2. *Hadamard products of D-finite series are D-finite.*
3. *Positive parts of D-finite series are D-finite.* □

Proof

1. This follows from

$$\begin{aligned}&\operatorname{diag}_{x_1,\dots,x_n} a(x_1,\dots,x_n,y_1,\dots,y_m)\\ &= \operatorname{Res}_{x_1,\dots,x_{n-1}} \frac{1}{x_1\cdots x_{n-1}} a\Big(x_1,\dots,x_{n-1},\frac{x_n}{x_1\cdots x_{n-1}},y_1,\dots,y_m\Big)\end{aligned}$$

(Exercise 8), the fact that D-finiteness of $a(x_1,\dots,x_n,y_1,\dots,y_m)$ implies D-finiteness of

$$\frac{1}{x_1\cdots x_{n-1}} a\Big(x_1,\dots,x_{n-1},\frac{x}{x_1\cdots x_{n-1}},y_1,\dots,y_m\Big),$$

and Theorem 5.31.
2. This follows from the previous part, because for any $a(x_1,\dots,x_n,y_1,\dots,y_m)$ and $b(x_1,\dots,x_n,z_1,\dots,z_\ell)$ we have

$$\begin{aligned}&a \odot_{x_1,\dots,x_n} b\\ &= \operatorname{diag}_{\bar{x}_1,x_1} \cdots \operatorname{diag}_{\bar{x}_n,x_n} a(x_1,\dots,x_n,y_1,\dots,y_m) b(\bar{x}_1,\dots,\bar{x}_n,z_1,\dots,z_\ell),\end{aligned}$$

where $\bar{x}_1,\dots,\bar{x}_n$ denote fresh variables (Exercise 8). Note that the product of a and b on the right hand side is well-defined because the variable sets are made disjoint.

3. This follows from the previous part, because for any $a(x_1,\dots,x_n,y_1,\dots,y_m)$ and the D-finite series

$$b = \frac{x_1 \cdots x_n}{(1-x_1)\cdots(1-x_n)} = \sum_{k_1,\dots k_n>0} x_1^{k_1} \dots x_n^{k_n},$$

we have

$$\begin{aligned}&[x_1^{>} \cdots x_n^{>}] a(x_1,\dots,x_n,y_1,\dots,y_m)\\ &= a(x_1,\dots,x_n,y_1,\dots,y_m) \odot_{x_1,\dots,x_n} b(x_1,\dots,x_n).\end{aligned}$$

■

Example 5.34 For the D-finite series $a(x,t) = \frac{1}{1-(x+x^{-1})t} = \sum_{n=0}^{\infty}(x+x^{-1})^n t^n$, we have

$$\begin{aligned}\operatorname{diag}_{x,t} a(x,t) &= [x^{-1}]x^{-1}a(x,t/x) = [x^{-1}]x^{-1}\sum_{n=0}^{\infty}(1+x^{-2})^n t^n\\ &= \sum_{n=0}^{\infty} t^n = \frac{1}{1-t},\\ a(x,t) \odot_{x,t} a(x,t) &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}x^{2k-n}t^n \odot_{x,t} \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}x^{2k-n}t^n\\ &= \frac{1}{\sqrt{1-(1+x)^2t/x}}\frac{1}{\sqrt{1-(1-x)^2t/x}},\\ [x^{>}]a(x,t) &= \sum_{n=0}^{\infty}[x^{>}]\sum_{k=0}^{n}\binom{n}{k}x^{2k-n}t^n = \sum_{n=0}^{\infty}\sum_{k=\lfloor n/2\rfloor+1}^{n}\binom{n}{k}t^n\\ &= \frac{2tx}{(1-4t^2)+\sqrt{1-4t^2}(1-2tx)}.\end{aligned}$$

The claimed algebraic expressions for these series can be proven by first computing annihilating operators for the left hand sides. This is done by reformulating the various expressions as residues and constructing a telescoper. Annihilating operators for the right hand sides can be obtained with the techniques of Sect. 3.3 if we view the series as elements of $C(x)[[t]]$. It then remains to compare the annihilating operators and to check a suitable number of initial values. □

Taking diagonals preserves D-finiteness, but does not preserve algebraicity or rationality. For example, the series $\operatorname{diag}_{x,y,z} \frac{1}{1-(x+y+z)} = \sum_{n=0}^{\infty} \frac{(3n)!}{n!^3} z^n$ is transcendental. So a natural question might be: which D-finite series do we obtain by taking diagonals of multivariate rational functions? It is known that the diagonal of a bivariate rational function is always algebraic (Exercise 9), and that every algebraic series is the diagonal of a rational function (Exercise 11). On the other hand, not every D-finite series is the diagonal of a rational function. For example, $\log(1-x) = -\sum_{n=1}^{\infty} \frac{1}{n} x^n$ is not a diagonal. The reason is that the denominators in the coefficients of a diagonal of a rational function can have at most finitely many different prime factors. More precisely, if $f \in \mathbb{Q}[[x]]$ is the diagonal of a multivariate rational function, then there exist $\alpha, \beta \in \mathbb{Q}$ such that $\alpha f(\beta x) \in \mathbb{Z}[[x]]$ (Exercise 15). Formal power series with this property are called *globally bounded*. Are there formal power series which are D-finite and globally bounded and which are not the diagonals of certain rational functions? Nobody knows, and it is an open conjecture due to Christol that there are none. In any case, the set of formal power series which are diagonals of rational functions forms an intermediate class between algebraic series and D-finite series.

Using Theorem 5.33, we can reduce definite sums with non-natural boundaries to definite sums with natural boundaries. Let $f(k_1, \ldots, k_m, n_1, \ldots, n_\ell)$ be a holonomic sequence and consider the definite sum

$$F(n_1, \ldots, n_\ell) = \sum_{(k_1,\ldots,k_m) \in \Omega_{n_1,\ldots,n_\ell}} f(k_1, \ldots, k_m, n_1, \ldots, n_\ell),$$

with finite summation ranges $\Omega_{n_1,\ldots,n_\ell} \subseteq \mathbb{Z}^m$ defined through linear inequalities with coefficients in $\mathbb{Q}$. More precisely, the requirement is that there are $\mathbb{Q}$-linear functions $p_1, \ldots, p_s \colon \mathbb{Q}^{m+\ell} \to \mathbb{Q}$ and rational numbers $\alpha_1, \ldots, \alpha_s \in \mathbb{Q}$ such that for all $n_1, \ldots, n_\ell \in \mathbb{Z}$ we have

$$\begin{aligned}(k_1, \ldots, k_m) \in \Omega_{n_1,\ldots,n_\ell} \iff\ & p_1(k_1, \ldots, k_m, n_1, \ldots, n_\ell) \geq \alpha_1 \\ & \vdots \\ & p_s(k_1, \ldots, k_m, n_1, \ldots, n_\ell) \geq \alpha_s.\end{aligned}$$

Geometrically, this means that for any fixed $n_1, \ldots, n_\ell \in \mathbb{Z}^m$, the set $\Omega_{n_1,\ldots,n_\ell}$ consists of the integer points of a polyhedron. Such sets are suitable as summation ranges because, as we have seen in Exercise 19 of Sect. 4.5, the functions $I_j \colon \mathbb{Z}^{m+\ell} \to \mathbb{Z}$ defined by

$$I_j(k_1, \ldots, k_m, n_1, \ldots, n_\ell) = \begin{cases} 1, & \text{if } p_j(k_1, \ldots, k_m, n_1, \ldots, n_\ell) \geq \alpha_j, \\ 0, & \text{otherwise,} \end{cases}$$

are holonomic. We can write the sum under consideration as

$$\begin{aligned}
&F(n_1,\dots,n_\ell)\\
&=\sum_{(k_1,\dots,k_m)\in\Omega_{n_1,\dots,n_\ell}} f(k_1,\dots,k_m,n_1,\dots,n_\ell)\\
&=\sum_{(k_1,\dots,k_m)\in\mathbb{Z}^m} f(k_1,\dots,k_m,n_1,\dots,n_\ell)\prod_{j=1}^{s} I_j(k_1,\dots,k_m,n_1,\dots,n_\ell).
\end{aligned}$$

The summand is holonomic by Theorem 5.33 and it has natural boundaries, so it follows from Theorem 5.24 that F is holonomic.

Example 5.35 The sum $F(n)=\sum_{k=0}^{n}\binom{k+n}{k}$ does not have natural boundaries. A holonomic annihilating ideal for $\binom{k+n}{k}$ is

$$\langle S_nS_k-S_n-S_k,\,(k+1)S_k-(n+k+1),\,(n+1)S_n-(n+k+1)\rangle\subseteq C[n,k][S_n,S_k].$$

A holonomic annihilating ideal for the function $I\colon\mathbb{Z}^2\to\mathbb{Z}$ defined by

$$I(n,k)=\begin{cases}1, & \text{if } k\le n,\\ 0, & \text{otherwise,}\end{cases}$$

is $\langle S_nS_k-1,\,kS_k-nS_n+n-k\rangle$. The holonomic annihilating ideal for the product $\binom{k+n}{k}I(n,k)$ contains the operator

$$(n+2)S_n-(4n+6)-(S_k-1)(2nS_n+kS_n-2n-6k),$$

so we find that $(n+2)S_n-(4n+6)$ is an annihilating operator for $F(n)$. □

If the summation range is as simple as in the previous example, an alternative way is to proceed in a similar way as in the integration case discussed at the beginning of the section. For example, for a sum $F(n)=\sum_{k=0}^{n} f(n,k)$, we would first find an annihilating operator $P-\Delta_k Q\in C[n,k][S_n,S_k]$ of $f(n,k)$ with $P\in C[n][S_n]\setminus\{0\}$ and then conclude that $P\cdot F(n)=(Q\cdot f)|_{k=n+1}-(Q\cdot f)|_{k=0}$. The term $(Q\cdot f)|_{k=0}$ is holonomic by Theorem 5.28. To see that $(Q\cdot f)|_{k=n+1}$ is holonomic as well, we need a theorem supporting this substitution. A first version of such a theorem was given in Theorem 4.72. The following alternative is based on taking residues. In Theorem 4.72, we made the assumption that the linear functions $g_1,\dots,g_n$ substituted into f should be linearly independent. Now we drop this assumption, but in order to be able to invoke D-finiteness results for generating functions, we need to impose restrictions on the supports of f and $f(g_1,\dots,g_n)$.

Theorem 5.36 *(See Theorem 5.30 for the differential case) Let $f\colon\mathbb{Z}^n\to C$ be a holonomic function (w.r.t. $C[x_1,\dots,x_n][S_{x_1},\dots,S_{x_n}]$). Let $g_1,\dots,g_n\colon\mathbb{Z}^m\to\mathbb{Z}$ be linear functions. Suppose that the supports of f and of $f(g_1,\dots,g_n)$*

belong to certain line-free polyhedral cones. Then the composition $f(g_1, \dots, g_n)$ is holonomic (w.r.t. $C[z_1, \dots, z_m][S_{z_1}, \dots, S_{z_m}]$). □

Proof Let $A = ((a_{i,j}))_{i,j=1}^{n,m} \in \mathbb{Z}^{n\times m}$ be the matrix such that

$$\begin{pmatrix} g_1(v_1, \dots, v_m) \\ \vdots \\ g_n(v_1, \dots, v_m) \end{pmatrix} = A \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}.$$

Since f is a holonomic function, the series

$$\sum_{k_1,\dots,k_n\in\mathbb{Z}} f(k_1, \dots, k_n) x_1^{k_1} \cdots x_n^{k_n} \in C_{\mathbb{Z}}[[x_1, \dots, x_n]]$$

is holonomic. By assumption on the support of f, it is then also D-finite. Then also

$$\sum_{\substack{k_1,\dots,k_n\in\mathbb{Z}\\ v_1,\dots,v_m\in\mathbb{Z}}} f(k_1, \dots, k_n) x_1^{k_1} \cdots x_n^{k_n} z_1^{v_1} \cdots z_m^{v_m} \in C_{\mathbb{Z}}[[x_1, \dots, x_n, z_1, \dots, z_m]]$$

is D-finite. By assumption on the support of $f(g_1, \dots, g_n)$, then also

$$\begin{aligned}&\sum_{\substack{k_1,\dots,k_n\in\mathbb{Z}\\ v_1,\dots,v_m\in\mathbb{Z}}} f(k_1, \dots, k_n) x_1^{k_1} \cdots x_n^{k_n} \Bigl(\frac{z_1}{\prod_{i=1}^n x_i^{a_{i,1}}}\Bigr)^{v_1} \cdots \Bigl(\frac{z_m}{\prod_{i=1}^n x_i^{a_{i,m}}}\Bigr)^{v_m} \\ &= \sum_{\substack{k_1,\dots,k_n\in\mathbb{Z}\\ v_1,\dots,v_m\in\mathbb{Z}}} f(k_1, \dots, k_n) x_1^{k_1-g_1(v_1,\dots,v_m)} \cdots x_n^{k_n-g_n(v_1,\dots,v_m)} z_1^{v_1} \cdots z_m^{v_m}\end{aligned}$$

is D-finite. Then also the residue of $(x_1 \cdots x_n)^{-1}$ times this series is D-finite. This is the series

$$\sum_{v_1,\dots,v_m\in\mathbb{Z}} f(g_1(v_1, \dots, v_m), \dots, g_n(v_1, \dots, v_m)) z_1^{v_1} \cdots z_m^{v_m}.$$

Therefore, $f(g_1, \dots, g_m)$ is holonomic. ■

As a special case of Theorem 5.36, we find again that the diagonal $(f(k, k, \dots, k))_{k=0}^{\infty}$ of a holonomic sequence $f: \mathbb{N}^n \to C$ is holonomic.

The next closure property is about symmetric functions. A power series $f \in C[[x_1, \dots, x_n]]$ is called *symmetric* if it is invariant under permuting its variables, i.e., if

$$f(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)})$$

for all permutations π. The concept extends to power series in infinitely many variables $x_1, x_2, \dots$. For example, the *power sums* $p_k := \sum_{i=1}^{\infty} x_i^k$ $(k \in \mathbb{N})$ are symmetric functions. More generally, a vector $\lambda = (\lambda_1, \dots, \lambda_m) \in \mathbb{N}^m$ is called an integer partition if $\lambda_1 \geq \cdots \geq \lambda_m > 0$, and for each such integer partition, we define $p_\lambda := p_{\lambda_1} \cdots p_{\lambda_m}$. It can be shown that these symmetric functions p_λ form a basis of the C-vector space of all symmetric functions in $x_1, x_2, \dots$. A scalar product $\langle\cdot|\cdot\rangle$ is defined on this vector space by setting

$$\langle p_\lambda | p_\mu \rangle = \delta_{\lambda,\mu} \prod_{k=1}^{\infty} k^{c_k} c_k!$$

for all partitions λ, μ. In this formula, c_k denotes the number of components of λ which are equal to k. As c_k is zero for almost all k, the product is in fact finite. Another operation is the so-called *internal product,* which is defined by

$$p_\lambda * p_\mu := p_\lambda \delta_{\lambda,\mu} \prod_{k=1}^{\infty} k^{c_k} c_k!.$$

We want to show that the scalar product and the internal product preserve D-finiteness. The scalar product maps two symmetric functions to an element of the ground field C, so in order for a D-finiteness statement to be meaningful in this case, we must replace C with a larger field involving some variables, e.g., $C_{\leq}((t_1, \dots, t_n))$. Another point that needs to be clarified is how we define D-finiteness for series with infinitely many variables. This is done as follows. We view a symmetric function f in $x_1, x_2, \dots$ as a power series in the "variables" $p_1, p_2, \dots$, and we say that such a power series is D-finite if for every finite subset $P \subseteq \{p_1, p_2, \dots\}$, the series obtained from f by setting all variables in $\{p_1, p_2, \dots\} \setminus P$ to zero is D-finite as series in the variables in P.

Theorem 5.37 *Let $f, g \in C_{\leq}((t_1, \dots, t_n))[[p_1, p_2, \dots]]$ be D-finite in $p_1, p_2, \dots$ and $t_1, \dots, t_n$.*

1. *$f * g$ is D-finite in $p_1, p_2, \dots$ and $t_1, \dots, t_n$.*
2. *If g involves only finitely many $p_1, p_2, \dots$, then $\langle f | g \rangle$ is D-finite in $t_1, \dots, t_n$.*

□

Proof

1. For the series $u = \sum_\lambda p_\lambda \prod_{k=1}^{\infty} k^{c_k} c_k!$ we have $f * g = (f \odot_{p_1, p_2, \dots} g) \odot_{p_1, p_2, \dots} u$ by definition of the internal product. It is therefore sufficient to show that u is D-finite. Because of

$$u = \sum_{c_1, c_2, \dots \in \mathbb{N}} \prod_{k=0}^{\infty} k^{c_k} c_k! p_k^{c_k} = \Big(\sum_{c_1 \in \mathbb{N}} c_1!(1p_1)^{c_1} \Big) \Big(\sum_{c_2 \in \mathbb{N}} c_2!(2p_2)^{c_2} \Big) \cdots ,$$

this follows from the D-finiteness of the series $\sum_{n=0}^{\infty} n!x^n$.

2. This follows from the first part by noting that $\langle f|g\rangle$ is obtained from $f * g$ by setting all p_k to 1. This substitution is legitimate by the assumption that g involves only finitely many p_k. The substitution also preserves D-finiteness because of Theorem 5.28. ■

The closure properties discussed in this section and elsewhere in this book are important for proving facts about D-finite functions. It is however worth keeping in mind that in order to prove a specific statement about some specific D-finite functions, it is not necessary to resort to general theorems that hold for all D-finite functions. There are situations where a quantity happens to be D-finite even though its D-finiteness does not follow in an obvious way from general closure properties. There is an interesting approach for proving identities about determinants which depends on the hope that an auxiliary quantity is D-finite. The approach succeeds if this is the case, and fails otherwise. The idea is as follows.

For a bivariate D-finite sequence $(a_{i,j})_{i,j=1}^{\infty}$, we consider the sequence $\Delta_n := \det((a_{i,j}))_{i,j=1}^{n}$ of the determinants of the $n \times n$ matrices whose entries are determined by the initial portion of the infinite sequence $(a_{i,j})_{i,j=1}^{\infty}$, i.e.,

$$\Delta_1 = a_{1,1}, \quad \Delta_2 = \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}, \ldots.$$

Let $(b_n)_{n=1}^{\infty}$ be another D-finite sequence with $b_n \neq 0$ for all $n \in \mathbb{N}$, for which it is conjectured that the identity

$$\Delta_n = \prod_{k=1}^{n} b_k$$

holds for all $n \in \mathbb{N}$. The goal is to prove this identity by induction on n. The base case is easy. For the induction step $n-1 \to n$, consider the linear system

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{pmatrix} v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

By induction hypothesis and the assumption $b_n \neq 0$, this system has a unique solution $v \in C^n$. Denote its coefficients by $c_{n,1}, \ldots, c_{n,n-1}$, and observe that $c_{n,j}$ is the quotient of the (n, j)th cofactor and the (n, n)th cofactor of the $n \times n$ matrix. Therefore, we have

$$\Delta_n = \Delta_{n-1} \sum_{j=1}^{n} c_{n,j} a_{n,j},$$

and the induction step is completed if we can show that the sum on the right hand side is equal to b_n.

There is no general reason to expect that the sequence $(c_{n,j})_{n,j=1}^{\infty}$ is D-finite, but if we are lucky and it is, then we can prove the required summation identity with a summation algorithm. Moreover, the definition of the $c_{n,j}$ as components of the solution vector of a linear system is equivalent to saying that the $c_{n,j}$ are the unique numbers satisfying the three identities

$$\begin{aligned} c_{n,n} &= 1 && (n \geq 1), \\ \sum_{j=1}^{n} c_{n,j} a_{i,j} &= 0 && (1 \leq i < n), \text{ and} \\ \sum_{j=1}^{n} c_{n,j} a_{n,j} &= b_n && (n \geq 1). \end{aligned}$$

We can therefore calculate many $c_{n,j}$ by solving the linear systems for various fixed n, apply multivariate guessing to find a candidate system of recurrence equations for the $c_{n,j}$, and then prove using summation algorithms that the sequence defined by the guessed recurrence equations satisfies these three identities. If this works, we have succeeded in proving the determinant identity, and the success depended on the sequence $c_{n,j}$ being kind enough to be D-finite even though no general closure property theorem forced it to be.

Example 5.38 In order to prove the identity

$$\det((\underbrace{\binom{x+i}{2j}}_{=:a_{i,j}}))_{i,j=1}^{n} = \prod_{k=1}^{n} \underbrace{\frac{x+k}{k} \frac{\left(\frac{x-k+1}{2}\right)^{\overline{k}}}{\left(\frac{3}{2}\right)^{\overline{k-1}}}}_{=:b_k} \qquad (n \in \mathbb{N}),$$

we compute the first few $c_{n,j}$ by solving the linear systems above. This gives

n/j	1	2	3	4	5
1	1	0	0	0	0
2	$-\frac{1}{12}(x-2)^{\overline{2}}$	1	0	0	0
3	$\frac{1}{360}(x-3)^{\overline{4}}$	$-\frac{1}{15}(x-3)^{\overline{2}}$	1	0	0
4	$-\frac{1}{20160}(x-4)^{\overline{6}}$	$\frac{1}{560}(x-4)^{\overline{4}}$	$-\frac{3}{56}(x-4)^{\overline{2}}$	1	0
5	$\frac{1}{1814400}(x-5)^{\overline{8}}$	$-\frac{1}{37800}(x-5)^{\overline{6}}$	$\frac{1}{840}(x-5)^{\overline{4}}$	$-\frac{2}{45}(x-5)^{\overline{2}}$	1

With a few more terms, it is not hard to guess the recurrences

$$\big(jS_j - 2(1+j)(1+2j)(j-n)\big)\cdot c_{n,j} \stackrel{?}{=} 0,$$
$$\big(2(j-n-1)(1+n)(1+2n)S_n - n\big)\cdot c_{n,j} \stackrel{?}{=} 0,$$

and from these, the closed form

$$c_{n,j} \stackrel{?}{=} \frac{(-4)^{j-1} j(-1)^{n+1}\left(\frac{3}{2}\right)^{\overline{j-1}}(n-j+1)^{\overline{j-1}}(x-n)^{\overline{2(n-j)}}}{n(2n-1)!}.$$

If we now define $\tilde{c}_{n,j}$ as the quantity on the right hand side, then we can prove, using summation algorithms, that

$$\tilde{c}_{n,n} = 1, \quad \sum_{j=1}^{n} \tilde{c}_{n,j} a_{i,j} = 0, \quad \text{and} \quad \sum_{j=1}^{n} \tilde{c}_{n,j} a_{n,j} = b_n,$$

for all $n \geq 1$ and all $i < n$. This proves that $\tilde{c}_{n,j} = c_{n,j}$ for all n, j, so the guessed equations as well as the determinant identity are correct. □

Exercises

1. The *convolution* of two functions $f, g\colon \mathbb{R} \to \mathbb{C}$ is defined as $h\colon \mathbb{R} \to \mathbb{C}$, $h(t) = \int_0^1 f(x)g(t-x)dx$. Show that convolution preserves D-finiteness.

2⋆. Let $(a_n)_{n=0}^{\infty}$ be a sequence in C and suppose that $\sum_k \binom{n}{k} a_k$ is D-finite. Show that $(a_n)_{n=0}^{\infty}$ is D-finite, too.

3. A *Riordan array* is a bivariate sequence $(a_{n,k})_{n,k=0}^{\infty}$ such that for certain power series $f, g \in C[[x]]$ we have $a_{n,k} = [x^k]fg^n$. For example, $a_{n,k} = \binom{n}{k}$ is a Riordan array via $f = 1$ and $g = x + 1$. Prove or disprove: If f and g are D-finite, then so is $(a_{n,k})_{n,k=0}^{\infty}$.

4. Show that every $p = D_{x_i} \in C[x_1, \ldots, x_n][D_{x_1}, \ldots, D_{x_n}]$ ($i \in \{1, \ldots, n\}$) meets the requirements of Lemma 5.19, and that the same is true for $p = \Delta_{x_i} = S_{x_i} - 1 \in C[x_1, \ldots, x_n][S_{x_1}, \ldots, S_{x_n}]$.

5⋆. Show that if $(a_{n,k})_{n,k=0}^{\infty}$ is holonomic with respect to $C[n, k][S_n, S_k]$, then the sequence $(a_{n,k}x^k)_{n,k=0}^{\infty}$ is holonomic with respect to $C[n, k, x][S_n, S_k, D_x]$.
Hint: Use the results of Exercise 5 in Sect. 4.5, Theorem 4.69, and Theorem 5.30.

6⋆. Why is $C((x, y)) = \bigcup_{e_1, e_2 \in \mathbb{Z}} x^{e_1} y^{e_2} C[[x, y]]$ not a field?

7. What is $[x^{>}]\frac{1}{x^3(x^2-x-1)}$?

8★★. Let $a \in C_{\mathbb{Z}}[[x_1, \ldots, x_n, y_1, \ldots, y_m]]$ and $b \in C_{\mathbb{Z}}[[x_1, \ldots, x_n, z_1, \ldots, z_\ell]]$. Show the following identities used in the proof of Theorem 5.33:

a. $\operatorname{diag}_{x_1,\ldots,x_n} a = \operatorname{Res}_{x_1,\ldots,x_{n-1}} \frac{1}{x_1\cdots x_{n-1}} a(x_1, \ldots, x_{n-1}, \frac{x_n}{x_1\cdots x_{n-1}}, y_1, \ldots, y_m)$.

b. $a \odot_{x_1,\ldots,x_n} b =$
$\operatorname{diag}_{\bar{x}_1,x_1} \cdots \operatorname{diag}_{\bar{x}_n,x_n} a(x_1, \ldots, x_n, y_1, \ldots, y_m)b(\bar{x}_1, \ldots, \bar{x}_n, z_1, \ldots, z_\ell)$.

9★. Let $f \in C[[x, y]]$ be rational, i.e., suppose that there are $p, q \in C[x, y] \setminus \{0\}$ such that $qf - p = 0$. Show that $\operatorname{diag}_{x,y} f$ is algebraic.

10★. What is wrong with the following argument? Since every rational function $f \in C(x, y)$ can be written as $f = a + \frac{b}{1+xc}$ for certain $a \in C(y)[x, x^{-1}]$ and $b, c \in C(y)[x]$, it follows that $\operatorname{Res}_x f = \operatorname{Res}_x a$ is not only algebraic, as proved in the previous exercise, but in fact rational.

11★★★. This exercise is about the algebraicity of residues of rational functions.

a. Let $m \in C[x, y]$ be irreducible and such that $y \mid m(0, y)$ and $y^2 \nmid m(0, y)$, so that there is a unique formal power series $a \in C[[x]]$ with $a(0) = 0$ and $m(x, a(x)) = 0$. Show that $a = \operatorname{Res}_y h$ for $h = \frac{yD_y \cdot m}{m}$ and an appropriate interpretation of h as a multivariate Laurent series.

b. The polynomial $m = y^2 - x^2(1 - x) \in C[x, y]$ has two distinct formal power series solutions a with $a(0) = 0$. Which of them (if any) appears as $\operatorname{Res}_y h$ for $h = \frac{yD_y \cdot m}{m}$ and a suitably chosen term order?

12. Show that the positive part of a univariate rational function is always rational but that the positive part of a bivariate rational function may be irrational.

13★★. This exercise is about the algebraicity of Hadamard products.

a. Let $a \in C[[x_1, \ldots, x_n]]$ be algebraic and $r \in C[[x_n]]$ be rational. Show that $a \odot_{x_n} r$ is algebraic. *Hint:* You may assume that C is algebraically closed.

b. Show that $[x^{\geq}y^{\geq}]\frac{1}{1-(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})t}$ is transcendental. Why is this not a contradiction to part a?

14. After Definition 5.32, we have remarked that the definition of the Hadamard product w.r.t. $x_1, \ldots, x_n$ of two series $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and $g(x_1, \ldots, x_n, z_1, \ldots, z_\ell)$ should also extend to the case where the variable sets $\{y_1, \ldots, y_m\}$ and $\{z_1, \ldots, z_\ell\}$ are not disjoint. Does Theorem 5.33 also extend to this case? For example, if $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and $g(x_1, \ldots, x_n, y_1, \ldots, y_m)$ are D-finite, is $f \odot_{x_1,\ldots,x_n} g$ also D-finite?

15★. Let $f \in \mathbb{Q}[[x]]$ be the diagonal of a rational series in n variables. Show that there are $\alpha, \beta \in \mathbb{Q} \setminus \{0\}$ such that $\alpha f(\beta x) \in \mathbb{Z}[[x]]$.

16★. Prove or disprove:

a. For any two power series $f, g \in C[[x_1, \ldots, x_n]]$ we have

$$\operatorname{diag}_{x_1,\ldots,x_n}(fg) = \operatorname{diag}_{x_1,\ldots,x_n}(f) \operatorname{diag}_{x_1,\ldots,x_n}(g).$$

b. $\operatorname{diag}_{x_1,x_2,x_3,x_4} f = \operatorname{diag}_{x_1,x_2} \operatorname{diag}_{x_3,x_4} f$ for every $f \in C_{\mathbb{Z}}[[x_1, x_2, x_3, x_4]]$.
c. If $f, g \in C[[x]]$ are diagonals of certain rational series in several variables, then so is their Hadamard product $f \odot_x g$.

17. The proof of Theorem 5.33 proceeds by reducing the computation of diagonals to that of residues, the computation of Hadamard products to that of diagonals, and the computation of positive parts to that of Hadamard products. Close the circle by providing a reduction from the computation of positive parts to that of residues.

18. Dyson's constant term identity states that for any choice $a_1, \ldots, a_n \in \mathbb{N}$ we have

$$[x_1^0 \cdots x_n^0] \prod_{1 \le i \ne j \le n} \Big(1 - \frac{x_i}{x_j}\Big)^{a_i} = \frac{(a_1 + \cdots + a_n)!}{a_1! \cdots a_n!}.$$

Prove this identity for $n = 2$.

19. (Nobuki Takayama) Prove or disprove:
a. $\sum_{n=0}^{\infty} \sum_{k=n^2}^{\infty} x^k y^n$ is D-finite.
b. $\sum_{n=0}^{\infty} \sum_{i,j:i^2+j^2 \le n^2} x^i y^j t^n$ is D-finite.

20. The nth elementary symmetric function $e_n \in C[[x_1, x_2, \ldots]]$ is defined as the sum of all monomials $x_{i_1} \cdots x_{i_n}$ with $i_1 < \cdots < i_n$. Express e_4 in terms of the power sum symmetric functions $p_1, p_2, \ldots$.

21. Prove that the symmetric functions $\prod_{i,j \in \mathbb{N}: i<j} (1+x_i x_j)$ and $\prod_{i,j \in \mathbb{N}: i<j} \frac{1}{1-x_i x_j}$ are D-finite.

22. Show that every power series $\sum_{n=0}^{\infty} a_n t^n \in C[[t]]$ can be written as the scalar product of two D-finite symmetric functions in infinitely many variables.

23. Check if the proof method described in this section works for Hilbert's determinant identity: $\det(H_n) = \prod_{k=1}^{n-1} \frac{k!^4}{(2k)!(2k+1)!}$, where $H_n = ((\frac{1}{i+j-1}))_{i,j=1}^n$.

References

In the theory of holonomic functions, evaluation at zero is a central operation. It is usually called *restriction* in this context and is viewed as an operation on D-modules. Further algebraic operations on D-modules can be interpreted as closure properties for holonomic functions, see [341] and the references there for some advanced operations and algorithms that we do not cover here.

Periods were introduced by Kontsevich and Zagier in [286]. The current knowledge about this class of numbers is limited.

Polyhedral regions appear in this section as summation ranges and as support of multivariate Laurent series. There is a theory about the integer points contained in such sets, which is nicely described in a book of Beck and Robins [46]. A more detailed introduction into fields of multivariate Laurent series can be found in a paper by Aparicio Monforte and Kauers [36]. An alternative approach is to consider towers of fields of univariate Laurent series, $C((x_1))((x_2))\cdots((x_n))$. This approach was taken by Xin [462]. Positive part extraction is also the main step of a calculus introduced by MacMahon [317] in the context of partition analysis. This approach was made algorithmic and promoted by Andrews, Paule and Riese [33, 34].

It has been recognized long ago that diagonals are interesting objects. Furstenberg showed in 1967 [199] that diagonals of bivariate rational functions are algebraic. In his paper from 1980 [412], Stanley reports as "private communication" that Zeilberger had shown the D-finiteness of the diagonal of any rational function. The first published proof of this fact may be due to Christol [147]. Lipshitz [313] showed that diagonals of D-finite functions are D-finite and observes that this also implies the closure under taking positive parts. In his other paper on D-finite functions [314], he draws the connection from diagonals to the Hadamard product and to definite integration. A more recent account on the relation between residues, Hadamard product, diagonals, and positive parts using the Laurent series was given in a paper on lattice walk counting by Bostan et al. in [94].

Theorem 5.30 appears as Proposition 2.3.(iii) in [314].

Christol's conjecture appears in [148, 149] and remains wide open. Not only is it unknown whether all globally bounded D-finite function are diagonals, it is not even known for certain specific examples whether they are. Bostan, Boukraa, Christol, Hassani, and Maillard [87, 89] give a list of challenges, of which only some have been settled so far [1, 79].

D-finiteness for symmetric functions was introduced by Gessel [212], who used the results of Lipshitz to prove the closure under internal product and scalar product. See [158] for a more constructive approach.

The approach described at the end of the section for proving determinant identities was suggested by Zeilberger [470]. It is great for proving lots of determinant identities that arise in enumerative combinatorics and elsewhere. Such identities have been collected by Krattenthaler [299, 300]. Examples of identities proven with the method include the q-TSPP theorem [293] as well as identities about rhombus tiling problems [176].

5.4 Creative Telescoping

Creative telescoping is an alternative technique for computing telescopers. In contrast to the approaches discussed in Sect. 5.2, which are all based on some sort of elimination, creative telescoping is based on indefinite summation/integration. Recall that $P \in C(n)[S_n]$ is a telescoper for f if there exists a $Q \in C(n,k)[S_n, S_k]$ such that for $g = Q \cdot f$ we have $P \cdot f = (S_k - 1) \cdot g$. In other words, g is the indefinite sum of $P \cdot f$. The telescoper P turns f, which may not be indefinitely summable, into an indefinitely summable term. The idea of creative telescoping is to make an ansatz $P = c_0 + c_1 S + \cdots + c_s S_n^s$ for a telescoper, where $c_0, \ldots, c_s$ are undetermined coefficients, and to apply an adjusted indefinite summation algorithm to $P \cdot f$. The algorithm is adjusted in such a way that it instantiates, if at all possible, the undetermined coefficients of P to make $P \cdot f$ summable.

Let us work out the required adjustment for the classical case where f is a hypergeometric term in n and k which we want to sum with respect to k. For any operator $P = c_0 + c_1 S_n + \cdots + c_s S_n^s$ we have that

$$\frac{P \cdot f}{f} = c_0 + c_1 \frac{S_n \cdot f}{f} + \cdots + c_s \frac{S_n^s \cdot f}{f}$$

is a rational function with $c_0, \ldots, c_s$ appearing only in its numerator. Therefore, writing $(S_k P \cdot f)/(P \cdot f)$ in Gosper form $\frac{\sigma_k(p)}{p} \frac{q}{\sigma_k(r)}$, the undetermined coefficients $c_0, \ldots, c_s$ will appear only in p but not in q or r (cf. Exercise 17 of Sect. 5.1). Following Gosper's algorithm, we next have to find a polynomial $y \in C(n)[k]$ such that

$$q\sigma_k(y) - ry = p,$$

where q and r are in $C(n)[k]$ and p is of the form $c_1 p_1 + \cdots + c_s p_s$ with $p_1, \ldots, p_s \in C(n)[k]$ and the still undetermined coefficients $c_0, \ldots, c_s$. In view of the presence of these unknowns on the right hand side, this equation is called the parameterized Gosper equation. Using the algorithms from Sect. 2.5, we can simultaneously solve this equation for $y \in C(n)[k]$ and $c_0, \ldots, c_s \in C(n)$. Any solution with $(c_0, \ldots, c_s) \neq 0$ translates into a solution of the creative telescoping problem. If there is no such solution, we increase the order s of the ansatz for P and try again.

Algorithm 5.39 *(Zeilberger)*
Input: *A bivariate hypergeometric term f, specified via the rational functions $(S_n \cdot f)/f$, $(S_k \cdot f)/f \in C(n, k)$.*
Output: *A nonzero operator $P \in C(n)[S_n]$ of minimal order and a rational function $Q \in C(n, k)$ such that $(P - (S_k - 1)Q) \cdot f = 0$.*

1 *for $s = 0, 1, 2, \ldots$, do*
2 *Make an ansatz $P = c_0 + c_1 S_n + \cdots + c_s S_n^s$ with undetermined coefficients $c_0, \ldots, c_s$.*
3 *Compute a Gosper form $\frac{\sigma_k(p)}{p} \frac{q}{\sigma_k(r)}$ of $\frac{S_k P \cdot f}{P \cdot f}$ and let $p_0, \ldots, p_s \in C(n)[k]$ be such that $p = c_0 p_0 + \cdots + c_s p_s$.*
4 *Use Algorithm 2.56 to find a basis of the solution space of $q\sigma_k(y) - ry = c_0 p_0 + \cdots + c_s p_s$.*
5 *if there is a solution $(y, c_0, \ldots, c_s) \in C(n)[k] \times C(n)^{s+1}$ with $(c_0, \ldots, c_s) \neq 0$, then*
6 *Pick such a solution and set $P = c_0 + \cdots + c_s S_n^s$.*

Set $Q = \begin{cases} \frac{ry}{p}\frac{P\cdot f}{f} & \text{if } p \neq 0, \\ 0 & \text{otherwise.} \end{cases}$

Return (P, Q).

Theorem 5.40 *Algorithm 5.39 is correct. It terminates if and only if a telescoper for f exists. In particular, it terminates whenever f is proper hypergeometric.* □

Proof It follows from the correctness of Gosper's algorithm that any output (P, Q) produced by Algorithm 5.39 is correct. Moreover, from the completeness of Gosper's algorithm (in combination with the correctness of Algorithm 2.56) it follows that Algorithm 5.39 cannot overlook any telescoper in the sense that if there is a telescoper P of order s, then the algorithm is guaranteed to find it and thus to terminate. Finally, every proper hypergeometric term is holonomic according to Theorem 5.14, and every holonomic summand admits a telescoper according to Theorem 5.24. Thus Algorithm 5.39 must terminate whenever the input is a proper hypergeometric term. ■

Example 5.41

1. For $f = \binom{n}{k}$ we have $\frac{S_n\cdot f}{f} = \frac{n+1}{n+1-k}$ and $\frac{S_k\cdot f}{f} = \frac{n-k}{k+1}$. For the choice $s = 0$, it would turn out that there is no solution, so let us directly consider $s = 1$. For undetermined c_0, c_1 and $P = c_0 + c_1 S_n$ we have

$$P\cdot f = \Bigl(c_0 + c_1\frac{n+1}{n+1-k}\Bigr)f$$

and

$$\frac{S_k P\cdot f}{P\cdot f} = \frac{c_0 + c_1\frac{n+1}{n-k}}{c_0 + c_1\frac{n+1}{n+1-k}}\,\frac{n-k}{k+1} = \frac{(n-k)c_0 + (n+1)c_1}{(n+1-k)c_0 + (n+1)c_1}\,\frac{n+1-k}{k+1},$$

so we obtain the parameterized Gosper equation

$$(n+1-k)\sigma_k(y) - ky = (n+1-k)c_0 + (n+1)c_1.$$

Its solution space in $C(n)[k]\times C(n)^2$ is generated by $(1, 2, -1)$, which translates into the telescoper $P = 2 - S_n$ and the certificate $Q = \frac{k}{n+1-k}$.

2. For $f = \binom{a}{k}\binom{b}{n-k}$ we have $\frac{S_n\cdot f}{f} = \frac{k-n+b}{n+1-k}$ and $\frac{S_k\cdot f}{f} = \frac{(k-a)(n-k)}{(k+1)(n-k-1-b)}$. We try again using $s = 1$. For undetermined c_0, c_1 and $P = c_0 + c_1 S_n$ we have

$$P\cdot f = \Bigl(c_0 + c_1\frac{k-n+b}{n+1-k}\Bigr)f$$

and

$$\frac{S_k P \cdot f}{P \cdot f} = \frac{c_0 + c_1 \frac{k+1-n+b}{n-k}}{c_0 + c_1 \frac{k-n+b}{n+1-k}} \frac{(k-a)(n-k)}{(k+1)(n-k-1-b)}$$
$$= \frac{(k-n)c_0 + (n-k-1-b)c_1}{(k-n-1)c_0 + (n-k-b)c_1} \frac{(k-a)(n+1-k)}{(k+1)(n-k-1-b)},$$

so we obtain the parameterized Gosper equation

$$(k-a)(n+1-k)\sigma_k(y) - k(n-k-b)y = (k-n-1)c_0 + (n-k-b)c_1.$$

Its solution space in $C(n)[k] \times C(n)^2$ is generated by $(-1, n-a-b, n+1)$, which translates into the telescoper $P = (n-a-b)+(n+1)S_n$ and the certificate $Q = \frac{k(k-n+b)}{k-n-1}$. □

The telescopers derived in the example above serve to prove the binomial theorem $\sum_k \binom{n}{k} = 2^n$ and the Vandermonde identity $\sum_k \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}$. Since their order s is equal to one, we can not only check the correctness of a conjectured closed form, but it is also particularly easy to find a hypergeometric closed form if no conjecture is available. If we obtain a higher order telescoper, we can use the algorithms of Sect. 2.6 to find its hypergeometric solutions, and use linear algebra to check if the definite sum under consideration can be written as a linear combination of them.

The order of annihilating operators found by creative telescoping may not be minimal. Even though we have shown in Theorem 5.40 that Algorithm 5.39 (as well as Algorithm 5.44) is guaranteed to find telescopers of minimal order, it must be observed that a telescoper of minimal order is not necessarily an annihilating operator of minimal order for the corresponding sum or integral. For example, the minimal order telescoper of the term $k\binom{n}{k}^2\binom{n}{2n+k}^3$ has order five, but since the sum $\sum_k k\binom{n}{k}^2\binom{n}{2n+k}^3$ is identically zero, it is annihilated by the operator 1, which has order zero. We have discussed similar phenomena in Sects. 2.3 and 3.3 in the context of closure properties, and we have seen there that if the order of a calculated annihilating operator is too large, we can find one of lower order by guessing and then proving its correctness using closure properties. In the present context, we can proceed in the same way. The unique monic telescoper of minimal order is called the *minimal telescoper.*

If there is a telescoper of order $s = 1$, an interesting symmetry between n and k becomes apparent if we rename the quantities in an appropriate way. If $P = c_0 + c_1 S_n$ and Q are such that $(P - (S_k - 1)Q) \cdot f = 0$, let h be a hypergeometric term with $P \cdot h = 0$, and define $\tilde{g} = (Q \cdot f)/(c_0 h)$ and $\tilde{f} = f/h$. Then we have

$$\tilde{f}_{n+1,k} - \tilde{f}_{n,k} = \tilde{g}_{n,k+1} - \tilde{g}_{n,k}.$$

A pair $(\tilde{f}, \tilde{g})$ of bivariate hypergeometric terms satisfying this equation is called a *WZ-pair.* Although we started out regarding k as the summation variable, the symmetry of the equation now allows us to change our viewpoint and sum with respect to n. If we have natural boundaries and there is no trouble with respect to singularities, we find that both $F_n = \sum_k \tilde{f}_{n,k}$ as well as $G_k = \sum_n \tilde{g}_{n,k}$ are constant (i.e., independent of n and k, respectively). For example, for $f = \binom{n}{k}$ we have

$$\tilde{f}_{n,k} = 2^{-n}\binom{n}{k} \quad \text{and} \quad \tilde{g}_{n,k} = \frac{k}{n+1-k}2^{-n}\binom{n}{k} = 2^{-n}\binom{n}{k-1},$$

so in addition to the binomial theorem $\sum_k 2^{-n}\binom{n}{k} = 1$ we find the extra identity $\sum_n 2^{-n}\binom{n}{k-1} = 2$. The two identities obtained from a WZ-pair are called *companion identities* (of each other).

Zeilberger's algorithm finds a first order telescoper for a surprisingly large number of definite hypergeometric sums that admit a hypergeometric closed form. It has better chances to find short telescopers than the algorithms described in Sect. 5.2, because it leaves some more freedom to the form of the certificate. Indeed, while algorithms based on elimination find (P, Q) in which not only P but also Q is free of k, or in which k appears only polynomially in Q, Zeilberger's algorithm is also capable of finding pairs (P, Q) where k may appear in the denominator of the certificate Q. Moreover, Zeilberger's search for a telescoper is exhaustive in the sense that if there is a telescoper of a certain order s, then the algorithm will find it. In particular, the algorithm finds a telescoper of smallest possible order. For the algorithms in Sect. 5.2, there is no such guarantee.

A downside of using rational function arithmetic rather than just polynomial arithmetic is that we may run into issues with singularities. When we sum over the creative telescoping relation, the rational function appearing in the certificate part is no longer viewed as an algebraic object but as an actual function. If there are singularities in the summation range, summing the creative telescoping relation is not meaningful. Unfortunately, such issues arise frequently in examples, but fortunately, they can often be easily repaired.

Example 5.42 Consider again the derivation of the binomial theorem $\sum_k \binom{n}{k} = 2^n$ discussed in the previous example. We have seen there that Zeilberger's algorithm finds the relation

$$2\binom{n}{k} - \binom{n+1}{k} = \frac{k+1}{n-k}\binom{n}{k+1} - \frac{k}{n+1-k}\binom{n}{k}.$$

In view of the denominators $n-k$ and $n+1-k$, it seems that for no specific $n \in \mathbb{N}$ we can let k run through all integers, because there are issues for $k = n$ and for $k = n+1$. However, if we "simplify" $\frac{k}{n+1-k}\binom{n}{k}$ to $\frac{k}{n+1}\binom{n+1}{k}$, we obtain the relation

$$2\binom{n}{k} - \binom{n+1}{k} = \frac{k+1}{n+1}\binom{n+1}{k+1} - \frac{k}{n+1}\binom{n+1}{k}.$$

After multiplying by $n+1$ we obtain an equation that is valid for all integers n, k. Note that $n+1$ does not depend on k, so it is no problem that it gets introduced into the coefficients of the telescoper. If we apply the summation operator $\sum_{k=0}^{n}$ to both sides, we find that $f(n) = \sum_{k=0}^{n} \binom{n}{k}$ satisfies the recurrence $2(n+1)f(n) - (n+1)f(n+1) = 0$, which is valid for all $n \in \mathbb{Z}$. □

Zeilberger's algorithm applies to definite hypergeometric sums and relies on Gosper's algorithm for hypergeometric indefinite summation. It has natural variants that apply to sums involving continuous parameters as well as to definite hyperexponential integrals involving either a discrete or a continuous parameter. For integrals, the Almkvist-Zeilberger algorithm introduced in Sect. 5.1 does the job of Gosper's algorithm. These variants are somewhat less important than Zeilberger's original version, because there are not as many interesting definite hyperexponential integrals as there are interesting definite hypergeometric sums. Rather than for evaluating integrals, the differential version of creative telescoping for rational and hyperexponential functions is used for executing the closure properties discussed in the previous section.

Example 5.43 In order to compute the residue $\operatorname{Res}_x \frac{1}{1-(x^2/t+t^2/x)}$, apply the differential version of Zeilberger's algorithm to the rational function $\frac{1}{1-(x^2/t+t^2/x)}$ to find the telescoper

$$P = -t^2(27t^3-4)D_t^2 - 3t(27t^3+2)D_t + 4$$

along with the certificate

$$Q = -\frac{-9t^7 + 18t^5x - 90t^4x^3 + 81t^3x^5 + 11t^3x^2 - 4tx^3 + 2x^5}{x(t^3 - tx + x^3)}.$$

The telescoper P is an annihilating operator for $\operatorname{Res}_x \frac{1}{1-(x^2/t+t^2/x)}$. Note that while the residue itself depends on the Laurent series ring in which the rational function $\frac{1}{1-(x^2/t+t^2/x)}$ is expanded, the telescoper is computed only using rational function arithmetic and therefore valid for every series interpretation. It is therefore not surprising that the telescoper is not always the minimal order annihilating operator for a particular series interpretation. The rational function in this example admits three different series expansions. For two of them the residue is zero, so the residue is annihilated by 1 in these cases. The third expansion has a residue for which P is an annihilating operator of minimal order. □

In order to cover more interesting examples in both the shift case and the differential case, as well as in various mixed cases, we turn to D-finite summands/integrands defined by higher order equations. In this more general situation, we can realize the idea of creative telescoping using Algorithm 5.8 of Sect. 5.1 in place of Gosper's algorithm. The resulting algorithm is known as Chyzak's algorithm.

Algorithm 5.44 *(Chyzak)*
Input: *An element f of a $C(x,t)[\partial_x, \partial_t]$-module M with $\dim_{C(x,t)} M < \infty$, where $C(x,t)[\partial_x, \partial_t]$ is an Ore algebra with $\sigma_x = \mathrm{id}$ or $\delta_x = 0$, and a constant β.*
Output: *A nonzero operator $P \in C(t)[\partial_t]$ and an element Q of M such that $P \cdot f = (\partial_x - \beta) \cdot Q$.*

1 *Let $e_1, \dots, e_r$ be a $C(x,t)$-vector space basis of M and let $A = ((a_{i,j}))_{i,j=1}^r \in C(x,t)^{r\times r}$ be such that $\partial_x \cdot e_j = \sum_{i=1}^r a_{i,j} e_i$ for $j = 1, \dots, r$.*
2 *for $s = 0, 1, 2, \dots$, do*
3 $\quad p_s = \begin{cases} f & \text{if } s = 0, \\ \partial_t \cdot p_{s-1} & \text{otherwise.} \end{cases}$
4 $\quad$ *if $\sigma_x = \mathrm{id}$ then*
5 $\quad\quad$ *Solve the coupled linear system*

$$A \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} + \begin{pmatrix} \delta(q_1) \\ \vdots \\ \delta(q_r) \end{pmatrix} - \beta \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = c_0 \begin{pmatrix} [e_1]p_0 \\ \vdots \\ [e_r]p_0 \end{pmatrix} + \dots + c_s \begin{pmatrix} [e_1]p_s \\ \vdots \\ [e_r]p_s \end{pmatrix}$$

for $q_1, \dots, q_r \in C(x,t)$ and $c_0, \dots, c_s \in C(t)$. Here, $[e_i]p_j$ refers to the coefficient of e_i in p_j.
6 $\quad$ *otherwise*
7 $\quad\quad$ *Solve the coupled linear system*

$$A \begin{pmatrix} \sigma(q_1) \\ \vdots \\ \sigma(q_r) \end{pmatrix} - \beta \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = c_0 \begin{pmatrix} [e_1]p_0 \\ \vdots \\ [e_r]p_0 \end{pmatrix} + \dots + c_s \begin{pmatrix} [e_1]p_s \\ \vdots \\ [e_r]p_s \end{pmatrix}$$

for $q_1, \dots, q_r \in C(x,t)$ and $c_0, \dots, c_s \in C(t)$.
8 $\quad$ *if there is a solution with $(c_0, \dots, c_s) \neq 0$ then*
9 $\quad\quad$ *Return $(c_0 + \dots + c_s \partial_t^s, q_1 e_1 + \dots + q_r e_r)$.*

The correctness and termination argument for Algorithm 5.44 is exactly the same as in Theorem 5.39.

Note that we have slightly adjusted the setting for the certificate; in this algorithm we view it as an element of the module M rather than as an operator. In the typical case when M is of the form $C(x,t)[\partial_x, \partial_t]/I$ for some ideal I, the difference is hardly more than cosmetic. In this case, $Q \in C(x,t)[\partial_x, \partial_t]$ is a certificate in the sense of Definition 5.18 if and only if its equivalence class is a certificate in the sense of the specification of Algorithm 5.44.

For an implementation of this algorithm, it should be taken into account that the matrix A defined in line 1 does not change during the iteration. If we use uncoupling to solve these systems, as explained in Sect. 4.3, we should arrange the computation in such a way that we need only a single call to the uncoupling algorithm. We can do this by computing, before entering the loop, a matrix $T \in C(x,t)[\partial_x, \partial_t]^{r\times r}$ such that $\tilde{A} := T(A - I_r\partial_x - \beta I_r)$ is uncoupled. (This is for $\sigma_x = \mathrm{id}$; otherwise choose T such that $\tilde{A} := T(A\partial_x - \beta I_r)$ is uncoupled.) For each s, we then only have to solve the uncoupled system

$$\tilde{A} \cdot \begin{pmatrix} q_1 \\ \vdots \\ q_r \end{pmatrix} = c_0 T \cdot \begin{pmatrix} [e_1]p_0 \\ \vdots \\ [e_r]p_0 \end{pmatrix} + \cdots + c_s T \cdot \begin{pmatrix} [e_1]p_s \\ \vdots \\ [e_r]p_s \end{pmatrix}$$

for $q_1, \ldots, q_r \in C(x,t)$ and $c_0, \ldots, c_s \in C(t)$.

Example 5.45

1. We want to compute the definite integral $F(n) = \int_{-1}^{1} P_n(x)^2 dx$, where $P_n(x)$ is the nth Legendre polynomial. We define a $C(n,x)[S_n, D_x]$-module structure on $M = C(n,x)^3$ by letting the unit vectors e_1, e_2, e_3 behave under shift and derivation like $P_n(x)^2$, $P_n(x)P_{n+1}(x)$, $P_{n+1}(x)^2$, respectively. This is an easy thing to do if we know the relations

$$(n+2)P_{n+2}(x) - (2n+3)xP_{n+1}(x) + (n+1) = 0,$$
$$(1-x^2)P_n'(x) + (n+1)P_{n+1}(x) - (n+1)x = 0.$$

For example, these equations imply $S_n \cdot e_2 = -\frac{n+1}{n+2}e_2 + \frac{(2n+3)x}{n+2}e_3$. Similarly, we obtain the matrix

$$A = \frac{n+1}{x^2-1}\begin{pmatrix} -2x & -1 & 0 \\ 2 & 0 & -2 \\ 0 & 1 & 2x \end{pmatrix}$$

in line 1 of the algorithm. Since we consider an integration problem, we choose $\beta = 0$. The main loop of the algorithm finds no solutions for $s = 0$. For $s = 1$, it finds that the coupled system

$$A\begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} - \begin{pmatrix} q_1' \\ q_2' \\ q_3' \end{pmatrix} = c_0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + c_1 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

has a nontrivial solution

$$(xe_1 - 2e_2 + xe_3, -2n-1, 2n+3) \in M \times C(t)^2.$$

This solution translates into the creative telescoping relation

$$\big((2n+3)S_n - (2n+1)\big) \cdot P_n(x)^2 = D_x \cdot \big(xP_n(x)^2 - 2P_n(x)P_{n+1}(x) + xP_{n+1}(x)^2\big).$$

We are lucky that there are no denominators in the certificate, so there are no issues with singularities. Integrating from -1 to 1 gives the equation $(2n+3)F(n+1)-(2n+1)F(n)=0$ for the integral $F(n)=\int_{-1}^{1}P_n(x)^2dx$.

2. Consider the sum $S(n)=\sum_k H_k\binom{n}{k}$, where H_k is the kth harmonic number. From the definition $H_k=\sum_{i=1}^{k}\frac{1}{i}$ and the defining recurrences for the binomial coefficient we can derive, using closure properties, the annihilating operators

$$\begin{aligned}&(n+1-k)S_n-(n+1) \quad \text{and}\\ &(k+2)^2S_k^2+(2k+3)(k+1-n)S_k+(k-n)(k+1-n)\end{aligned}$$

for the summand $f(n,k)=H_k\binom{n}{k}$. Let I be the ideal generated by these two operators in $C(n,k)[S_n,S_k]$, and let $M=C(n,k)[S_n,S_k]/I$. The module M is generated by the equivalence classes $e_1:=[1]$ and $e_2:=[S_k]$. In line 1 of the algorithm, we find the matrix

$$A=\begin{pmatrix}0 & (n-k)(k+1-n)/(k+2)^2\\ 1 & -(2k+3)(k+1-n)/(k+2)^2\end{pmatrix}.$$

Since we consider a summation problem, we choose $\beta=1$. There is no telescoper of order 0 or 1. In the iteration for $s=2$, we have to solve the coupled system

$$A\begin{pmatrix}\sigma_k(q_1)\\ \sigma_k(q_2)\end{pmatrix}-\begin{pmatrix}q_1\\ q_2\end{pmatrix}=c_0\begin{pmatrix}1\\0\end{pmatrix}+c_1\begin{pmatrix}-\frac{n+1}{n+1-k}\\ 0\end{pmatrix}+c_2\begin{pmatrix}\frac{(n+1)(n+2)}{(n+1-k)(n+2-k)}\\ 0\end{pmatrix}.$$

Its solution

$$\Big(\frac{(n+1)(3k^2-3k-n-2kn-2)}{(k-n-2)(k-n-1)}+\frac{(k+1)^2(n+1)}{(k-n)(k-n-1)}S_k,\\ -4(n+1),-2(2n+3),n+2\Big)$$

in $M\times C(n)^3$ translates into the creative telescoping relation

$$\begin{aligned}&\big((n+2)S_n^2-2(2n+3)S_n-4(n+1)\big)\cdot f(n,k)\\ &=\Delta_k\cdot\Big(\frac{(n+1)(3k^2-3k-n-2kn-2)}{(k-n-2)(k-n-1)}f(n,k)\\ &\qquad+\frac{(k+1)^2(n+1)}{(k-n)(k-n-1)}f(n,k+1)\Big)\\ &=\Delta_k\cdot\Big(\frac{3k^2-3k-n-2kn-2}{n+2}H_k\binom{n+2}{k}+\frac{(k+1)^2}{n+2}H_{k+1}\binom{n+2}{k+1}\Big).\end{aligned}$$

Summing over k and observing that the sum has natural boundaries, we find the recurrence

$$(n+2)S(n+2) - 2(2n+3)S(n+1) - 4(n+1)S(n) = 0. \qquad \square$$

The creative telescoping algorithms discussed so far extend easily to summation/integration problems with several free parameters. In this case, creative telescoping can be combined with FGLM (Algorithm 4.73) in order to obtain a basis of the ideal of telescopers. Recall from Sect. 5.2 that in this case, the certificate consists of a tuple of operators, one for each generator of the ideal.

Example 5.46 In the previous example, we have assumed that the Legendre polynomials are defined in terms of given annihilating operators. Another way to define them is via $P_n(x) = \sum_k \binom{n}{k}\binom{n+k}{k}\left(\frac{x-1}{2}\right)^k$. Using Zeilberger's algorithm in combination with FGLM, we can find the following telescopers, along with the corresponding certificates:

$$P_1 = (n+2)S_n^2 - (2n+3)xS_n + (n+1), \quad Q_1 = -\frac{2k^2(2n+3)}{(k-n-2)(k-n-1)},$$

$$P_2 = (n+1)S_n + (1-x^2)D_x - (n+1)x, \quad Q_2 = \frac{2k^2}{x-1}.$$

Indeed, the two operators P_1, P_2 are precisely the operators we used in the example above. They generate the annihilating ideal of $P_n(x)$ in $C(x,n)[D_x, S_n]$. $\square$

While the extension of creative telescoping to more than one parameter is straightforward, the extension to several summation/integration variables is less obvious. Recall that this situation also leads to certificates consisting of several components, one for each summation/integration variable. For example, for computing a double sum of a function $f(n,i,j)$ with respect to i and j, we would need an operator $P \in C(n)[S_n] \setminus \{0\}$ and two operators $Q_1, Q_2 \in C(n,i,j)[S_n, S_i, S_j]$ such that

$$P - \Delta_i Q_1 - \Delta_j Q_2 \in \operatorname{ann}(f).$$

Then P is a telescoper for f and its certificate is the pair (Q_1, Q_2). As indefinite summation/integration is an inherently univariate matter and creative telescoping rests on indefinite summation/integration, it is not clear how to find such relations directly using a creative telescoping approach. In fact, little is known about the multivariate indefinite summation/integration problem, which asks for deciding whether or not a given ℓ-variate function f of a certain type (e.g., a hypergeometric term) can be written in the form $f = \Delta_1 g_1 + \cdots + \Delta_\ell g_\ell$ for some $g_1, \ldots, g_\ell$. It seems that progress towards a creative telescoping algorithm for multiple definite sums/integrals requires a better understanding of this problem.

On the other hand, this does not mean that we have to fall back to the expensive elimination-based techniques discussed in Sect. 5.2 in order to handle a multiple sum/integral. We can still apply creative telescoping repeatedly, handling one summation/integration variable at a time. This is quite a natural idea: in order to find a recurrence for $\sum_{i,j} f(n,i,j)$, we first find a system of recurrences for the sum $F(n,i) = \sum_j f(n,i,j)$ by creative telescoping, and then use creative telescoping once more to find a recurrence for $\sum_i F(n,i)$. But what happens to the certificates in this approach? The call to creative telescoping for the outer sum produces certificates with respect to the inner sum $F(n,i)$, while we would probably prefer certificates in terms of the original summand $f(n,i,j)$.

Fortunately, the certificates with respect to $F(n,i)$ can be translated into certificates with respect to $f(n,i,j)$. This works as follows. Suppose that for the summand $f(n,i,j)$ we have found telescopers $P_1,\dots,P_m \in C(n,i)[S_n,S_i]$ along with certificates $Q_1,\dots,Q_m \in C(n,i,j)[S_n,S_i,S_j]$. This means that $P_1 - \Delta_j Q_1,\dots,P_m - \Delta_j Q_m$ belong to the annihilating ideal of $f(n,i,j)$. Next, apply creative telescoping to the element $f = 1$ of the module $M = C(n,i)[S_n,S_i]/\langle P_1,\dots,P_m\rangle$, and suppose this returns a telescoper $P \in C(n)[S_n]$ with a certificate $Q \in C(n,i)[S_n,S_i]$. This means that $P - \Delta_i Q$ is an element of $\langle P_1,\dots,P_m\rangle$. Using Gröbner bases, we can find $R_1,\dots,R_m \in C(n,i)[S_n,S_i]$ such that

$$P - \Delta_i Q = R_1 P_1 + \cdots + R_m P_m.$$

This is an equality in $C(n,i)[S_n,S_i]$, but we may as well read it as an equality in $C(n,i,j)[S_n,S_i,S_j]$ that happens to be free of j and S_j. We can then subtract $\Delta_j(R_1 Q_1 + \cdots + R_m Q_m)$ from both sides to find that

$$P - \Delta_i Q - \Delta_j(R_1 Q_1 + \cdots + R_m Q_m) = R_1(P_1 - \Delta_j Q_1) + \cdots + R_m(P_m - \Delta_j Q_m).$$

Note that $R_1,\dots,R_m$ commute with $\Delta_j = S_j - 1$ because they are free of j. Since the right hand side belongs to the annihilator of $f(n,i,j)$, so does the left hand side. This is the desired telescoper-certificate pair for $f(n,i,j)$. Of course, the construction generalizes to problems with more than two summation/integration variables or more than one free parameter.

Example 5.47 For $f(n,i,j) = \binom{n+j}{2i}\binom{i}{j}$, consider the double sum

$$F(n) = \sum_i \sum_j f(n,i,j).$$

For the summation with respect to j, Zeilberger's algorithm finds the following telescopers and certificates:

$$P_1 = (1 + 3i - 2n)(i - 1 - n)S_n - 4(1 + i)(1 + 2i)S_i$$

$$\begin{aligned}
&\quad + (1 + 5i + 8i^2 - n - 7in + 2n^2),\\
Q_1 &= -\frac{j(i^2 + ij - 4in - 4i + j + 2n^2 + 2n - 1)}{i - j + 1},\\
P_2 &= (2 - i + n)S_n^2 - (3i + 1)S_n - (n + 1),\\
Q_2 &= \frac{2ij}{n + j + 1 - 2i}.
\end{aligned}$$

Let I be the ideal generated by P_1, P_2 in $C(n,i)[S_n, S_i]$ and let $M = C(n,i)[S_n, S_i]/I$. Chyzak's algorithm applied to the element $f = 1$ of this module gives the pair

$$P = S_n - 3, \quad Q = \frac{i - 2n - 1}{n}S_n + \frac{2n + 3i + 1}{n}.$$

For

$$R_1 = \frac{(i - 2n)}{4(i + 1)(2i + 1)n}S_n + \frac{3i + 2n + 4}{4(i + 1)(2i + 1)n} \text{ and } R_2 = \frac{(i - 2n)(3i - 2n - 1)}{4(i + 1)(2i + 1)n},$$

we have $P - (S_i - 1)Q = R_1P_1 + R_2P_2$. A certificate of P therefore consists of Q and $\tilde{Q} = R_1Q_1 + R_2Q_2$. The operators Q and $\tilde{Q}$ can be simplified by adding arbitrary elements of the annihilating ideal of $f(n, i, j)$ to them. In particular, we can replace them by their normal form with respect to a Gröbner basis of the annihilating ideal. The resulting creative telescoping relation is then

$$\left((S_n - 3) - \Delta_i \frac{2i(3i - 2j - 1)}{n(2i - j - n - 1)} - \Delta_j \frac{j(ij - in - 3i + j - 1)}{(2i + 1)n(i - j + 1)}\right) \cdot f(n, i, j) = 0.$$

Indeed, we have $F(n + 1) - 3F(n) = 0$ for $n > 1$. $\square$

The lack of an indefinite summation/integration algorithm for the multivariate case is equivalent to the lack of a guarantee that the telescopers found by repeated application of univariate creative telescoping algorithms have minimal order. In general, this approach yields nonminimal telescopers. Nonminimal telescopers can also be found in other ways. One idea is to enhance the linear algebra approach discussed in Sect. 5.2. There, we searched for an annihilating operator of the summand/integrand whose coefficients do not involve the summation/integration variables, and then turned this operator into a creative telescoping relation. We can hope to go along with a smaller linear system if we take into account, like in the example above, that the certificates can always be brought into normal form with respect to the annihilating ideal I of the summand/integrand to the certificate. So for the ansatz of the certificate it suffices to take into account the terms that are irreducible ("under the staircase") with respect to a Gröbner basis of I. We must not expect that the elements of I that we add to a certificate to bring it into normal form are also free of the summation/integration variables, so restricting the terms in the ansatz only has a chance to work if we modify the ansatz to allow the summation/integration variables to appear.

These variables appear as rational functions, and we cannot simply make an ansatz for the coefficients of their numerator and denominator because this would lead to a nonlinear system and solving such systems is too expensive. If someone would tell us the denominators that can appear in the certificate so that we would only need to make an ansatz for the numerators, then we would just have to solve a linear system. In fact, there is a way to predict the denominators in the certificate. Recall that we started from an annihilating operator not involving the summation variables and then observed that the certificates can be reduced with respect to a Gröbner basis. The denominators which can get introduced in this process are determined by the denominators of the elements of the Gröbner basis. We might not know in advance how many factors are needed, nor what the degrees of the numerator are, but if we make a sufficiently generous choice, we will surely find something. This is the idea behind the following algorithm. In the interest of readability, we formulate it for the case of one summation/integration variable x and one free parameter t, but unlike the algorithms of Zeilberger and Chyzak, it extends easily to the case of several summation/integration variables.

Algorithm 5.48 *(Koutschan)*
Input: *An element f of a $C(x,t)[\partial_x,\partial_t]$-module M whose dimension as a $C(x,t)$-vector space is finite.*
Output: *$P \in C(t)[\partial_t] \setminus \{0\}$ and $Q \in M$ such that $P \cdot f = \partial_x \cdot Q$.*

1 *Let $e_1,\dots,e_r$ be a $C(x,t)$-vector space basis of M.*
2 *for $s = 0,1,2,\dots,$ do*
3 *Find a polynomial $b \in C(t)[x]$ such that the coefficients of $b\partial_x^i\partial_t^j \cdot f$ with respect to $e_1,\dots,e_r$ are in $C(t)[x]$, for all i,j with $0 \le i+j \le s$.*
4 *With undetermined coefficients c_i and $q_{i,j}$, compute*

$$u = \sum_{i=0}^{s} c_i\partial_t^i \cdot f - \partial_x \cdot \frac{1}{b}\sum_{i=0}^{s+\deg_x(b)}\sum_{j=1}^{r} q_{i,j}x^i e_j.$$

5 *Let $d \in C(t)[x] \setminus \{0\}$ be the common denominator of the coefficients of u with respect to $e_1,\dots,e_r$, equate the coefficients of du with respect to $x^i e_j$ to zero, and solve the resulting linear system over $C(t)$.*
6 *If there is a solution for which at least one c_i is nonzero, return the operator $P = \sum_{i=0}^{s} c_i\partial_t^i$ and the module element $Q = \frac{1}{b}\sum_{i=0}^{s+\deg_x(b)}\sum_{j=1}^{r} q_{i,j}x^i e_j$ corresponding to this solution.*

Theorem 5.49 *Algorithm 5.48 is correct. Moreover, if $C[x,t][\partial_x,\partial_t]$ is an Ore algebra such that $\sigma_x(x) \in C[x]$ and for ∂_x the polynomial x meets the requirements of Lemma 5.19, and if the annihilator of f in $C[x,t][\partial_x,\partial_t]$ is a holonomic ideal, then the algorithm terminates for the input f.* □

Proof Since $e_1, \ldots, e_r$ is a $C(x,t)$-vector space basis of M and d is chosen in line 5 such that du has coefficients in $C(t)[x]$, and since the powers of x form a $C(t)$-vector space of $C[x]$, we have that du is zero if and only if all its coefficients with respect to $x^i e_j$ are zero. It follows that for P and Q constructed in line 6 we have $P \cdot f = \partial_x \cdot Q$. This implies the correctness.

For the termination, observe that the additional assumptions are such that Theorem 5.24 implies the existence of an element $L \in C[x,t][\partial_x, \partial_t]$ with $L \cdot f = 0$ which can be written in the form $P - \partial_x \tilde{Q}$ for some $P \in C[t][\partial_t] \setminus \{0\}$ and some $\tilde{Q} \in C[x,t][\partial_x, \partial_t]$. For such an L, consider $Q = \tilde{Q} \cdot f \in M$. The coefficients of Q with respect to $e_1, \ldots, e_r$ are elements of $C(x,t)$, and for all sufficiently large s, their denominators will divide b, so that bQ will have coefficients in $C(t)[x]$ for these s. Their degrees with respect to x will depend on b, because b may have more factors than necessary, but if $b_0 \in C(t)[x]$ is the least common denominator of the coefficients of Q and $\delta \in \mathbb{N}$ is a bound on the degrees of the coefficients of $b_0 Q$ with respect to x, then the degrees of the coefficients of bQ with respect to x are bounded by $\delta + \deg_x(b)$. Therefore, for all sufficiently large s, we can write Q in the form $\frac{1}{b} \sum_{i=0}^{s+\deg_x(b)} \sum_{j=1}^{r} q_{i,j} x^i e_j$ for certain $q_{i,j} \in C(t)$. Finally, for all sufficiently large s, we also have $s \geq \deg_{\partial_t} P$. We have therefore shown that the loop counter will eventually be large enough so that a pair (P, Q) with the desired properties is found. ∎

Example 5.50 Consider again the hypergeometric term $f(n,i,j) = \binom{n+j}{2i}\binom{i}{j}$ from Example 5.47. Its annihilating ideal in $C(n,i,j)[S_n, S_i, S_j]$ is generated by

$$\begin{aligned} G = \big\{&(j+1)(2i-j-n-1)S_j + (i-j)(j+n+1),\\ &2(2i+1)(i-j+1)S_i - (2i-j-n)(2i-j-n+1),\\ &(2i-j-n-1)S_n + (j+n+1)\big\}. \end{aligned}$$

A natural choice for M is $C(n,i,j)[S_n, S_i, S_j]/\langle G \rangle$. We can choose $e_1 = 1$ as a generator. For $s = 0$, the algorithm finds no solutions. For $s = 1$, the least common denominator of the normal forms of the terms $1, S_n, S_i, S_j$ with respect to G is $b = (2i+1)(2i-j-n-1)(i-j+1)(j+1)$. This is slightly pessimistic. It turns out that the factor $j+1$ is not needed. In order to get smaller expressions, let us assume we know this and take $b = (2i+1)(2i-j-n-1)(i-j+1)$ instead. We make the ansatz

$$u = (c_0 + c_1 S_n) \cdot f - (S_i - 1) \cdot \frac{1}{b} \sum_{0 \leq u+v \leq 4} q_{u,v} i^u j^v - (S_j - 1) \cdot \frac{1}{b} \sum_{0 \leq u+v \leq 4} \tilde{q}_{u,v} i^u j^v.$$

Writing u in terms of the basis of M amounts to computing a normal form with respect to G. The result is a rational function in i, j, n. Equating the coefficients of the numerator to zero gives a linear system over $C(n)$ with 44 equations and 32 variables. The solution space of this system has dimension two. One solution corresponds to the operator

$$(S_n - 3) - \Delta_i \frac{2i(3i - 2j - 1)}{n(2i - j - n - 1)} - \Delta_j \frac{j(ij - in - 3i + j - 1)}{(2i + 1)n(i - j + 1)}$$

which we already found earlier. Another solution corresponds to the operator

$$\begin{aligned} 0 + \Delta_i &\frac{2(3ij + in + i - 2j^2 - 2jn - 2j)}{2i - j - n - 1} \\ -\Delta_j &\frac{j(4in + 4i - j^2 - 2jn - j - n^2 + n + 2)}{(2i + 1)(i - j + 1)} \end{aligned}$$

and is not useful for our purpose because its telescoper part is zero. □

The performance of Algorithm 5.48 depends crucially on an optimized implementation. Usually, the algorithm will need a number of iterations before it encounters a linear system with a nontrivial solution. In the search phase, homomorphic images should be used for checking whether a system is solvable, i.e., parameters should be set to constants, and the constant field should be mapped to a finite field. In such a homomorphic image, the cost of solving a linear system is negligible. Once a system is found to have a solution, we have to solve it again over $C(t)$, or apply interpolation and rational reconstruction techniques, in order to find P and Q. This step is the bottleneck of the whole computation, and the optimizations should focus on keeping this final linear system as small as possible.

Once a relation has been detected, we can check whether some of the factors were unnecessary, by going through the irreducible factors of the common denominator and checking for each factor whether the ansatz also succeeds without the selected factor. A more aggressive variant applies this optimization not only to the common denominator b of u but optimizes the denominator of each coefficient of u separately. This variant has to do a lot more trials, and although this may lead to considerably smaller denominators, the additional work required for identifying them does not always pay off. After the denominator optimization has been completed, we optimize the numerators. This is much easier: we simply discard every term $x^i e_j$ from the ansatz whose coefficient $q_{i,j}$ has zero in the homomorphic image. If the finite field is not too small, it is unlikely that the homomorphic image of a nonzero coefficient is zero.

Besides optimizing the shape of the ansatz, we can improve the efficiency of Algorithm 5.48 by avoiding some unnecessary recomputations. For example, if we precompute a matrix $A = ((a_{i,j}))_{i,j=1}^r \in C(x,t)^{r \times r}$ such that $\partial_x \cdot e_j = \sum_{i=1}^r a_{i,j} e_i$ for all j, like in Algorithm 5.44, we can use this matrix to compute $\partial_x \cdot \frac{1}{b} \sum_{i=0}^{s+\deg_x(b)} \sum_{j=1}^r q_{i,j} x^i e_j$. For the terms corresponding to the telescoper, we can reuse the terms $\partial_t \cdot f, \ldots, \partial_t^{s-1} \cdot f$ from the previous iteration and compute the new term via $\partial_t^s \cdot f = \partial_t \cdot (\partial_t^{s-1} \cdot f)$.

Another point to take into account are solutions of systems that do not give rise to a nonzero telescoper. Such solutions arise primarily in the case of several summation/integration variables, where they indicate relations among the components of the certificate. We have seen such a relation in the example above. If we integrate with respect to x_1, x_2, we systematically have $\partial_{x_1}\partial_{x_2} - \partial_{x_2}\partial_{x_1} = 0$, and this relation will show up among the solutions of a linear system if $\partial_{x_2}, \partial_{x_1}$ are among the basis elements $e_1, \ldots, e_r$. If we encounter such a relation, we should adjust the ansatz to ensure that it does not show up again in subsequent iterations.

Exercises

1. Evaluate once more the definite hypergeometric sums of Exercise 10 in Sect. 5.2, now via creative telescoping.

2. Evaluate once more the definite integrals of Exercises 11 and 13 in Sect. 5.2, now via creative telescoping.

3. Check the proof of Vandermonde's identity in Example 5.41 for possible issues with poles, and if there are any, fix them.

4. Let h be a bivariate hypergeometric term. Prove or disprove: The certificate of a telescoper of h can only be zero if h is constant with respect to one of the variables.

5. Algorithm 5.39 includes a special handling of the case where the certificate is zero. Can it also happen that the parameterized Gosper equation $q\sigma_k(y) - ry = p$ has a nonzero solution $(y, c_0, \ldots, c_s)$ with $c_0 = \cdots = c_s = 0$?

6. Prove or disprove: If a hypergeometric term h admits a telescoper of order s, then so does the term kh.

7. Show that for every fixed $m \in \mathbb{N}$, the hypergeometric term $h = (-1)^k\binom{n}{k}\binom{mn+k}{k}$ admits a telescoper of order 1.

8. Show that for every fixed $m \in \mathbb{N}$, the hypergeometric term $h = \binom{n}{mk}$ admits a telescoper with constant coefficients.

9*. Derive the companion identity of $\sum_k \frac{(-1)^k}{k+1}\binom{2k}{k}\binom{n+k}{2k+1} = 1$ $(n > 1)$.

10. Suppose that two hypergeometric terms $f(n,k)$ and $g(n,k)$ form a WZ-pair, and let $\tilde{f}(n,k) = g(-k-1,-n)$ and $\tilde{g}(n,k) = f(-k,-n-1)$. Show that $\tilde{f}(n,k)$ and $\tilde{g}(n,k)$ also form a WZ-pair.

11*. (Peter Paule and Markus Schorn) Show that for every hypergeometric term h (in one variable) there exists a nonzero polynomial p such that ph is indefinitely summable.

12. (George Boros and Victor Moll) Show that for every polynomial p there is a polynomial q such that $\sum_k p(k)\binom{n}{k} = q(n)2^n$.

13. It was claimed in Example 5.43 that the rational function $\frac{1}{1-(\frac{x^2}{t}+\frac{t^2}{x})}$ has two series expansions for which the residue with respect to x is zero. Check this.

14. Gauss famously evaluated the sum $\sum_{k=0}^{n} k$ as a child by observing that $\sum_{k=0}^{n} k = \sum_{k=0}^{n}(n-k)$ implies $2\sum_{k=0}^{n} k = \sum_{k=0}^{n} k + \sum_{k=0}^{n}(n-k) = \sum_{k=0}^{n} n = n(n+1)$. In a similar vein, Paule observed that sometimes a hypergeometric definite sum $\sum_{k=0}^{n} h(n,k)$ has a telescoper of higher order than the sum $\sum_{k=0}^{n}\bigl(h(n,k) + h(n,n-k)\bigr)$. Find an example where this is the case.

15⋆. In part 1 of Example 5.45, check that the right hand side of the creative telescoping relation evaluates to zero when we do the integration.

16⋆⋆⋆. (Neil Calkin) Find a closed form for $\sum_{k=0}^{n}\Bigl(\sum_{i=0}^{k}\binom{n}{i}\Bigr)^3$.

17⋆⋆⋆⋆. (Roger Apéry) Show that the sum $\sum_k \binom{n}{k}^2\binom{n+k}{k}^2$ satisfies a recurrence of order two, and that

$$\sum_k \binom{n}{k}^2\binom{n+k}{k}^2\Biggl(\sum_{i=1}^{n}\frac{1}{i^3} - \sum_{i=1}^{k}\frac{(-1)^i}{2i^3\binom{n}{i}\binom{n+i}{i}}\Biggr)$$

is also a solution of this recurrence.

18. Let $I \subseteq C(x,t)[\partial_x,\partial_t]$ be a D-finite ideal, and let T be the telescoping ideal for I with respect to x. Prove or disprove:

a. We always have $\dim_{C(t)} C(t)[\partial_t]/T \le \dim_{C(x,t)} C(x,t)[\partial_x,\partial_t]/I$.

b. We always have $\dim_{C(x,t)} C(x,t)[\partial_x,\partial_t]/I \le \dim_{C(t)} C(t)[\partial_t]/T$.

19. (Victor Moll) For $n \in \mathbb{N}$ and $t > -1$ real, let $I(n,t) = \int_0^\infty \frac{1}{(x^4+2tx^2+1)^{n+1}}dx$.

a. Derive a recurrence for $I(n,t)$ with respect to n.

b. Derive a differential equation for $I(n,t)$ with respect to t.

20⋆. (Ha Le) Let $a, b \in \mathbb{Z}$, $c \in C$, $m \in \mathbb{N}\setminus\{0\}$, $f = 1/(an+bk+c)^m \in C(n,k)$, and suppose that $b > 0$. Show that $P = S_n^b - 1$ is a telescoper for f.

21⋆. We have remarked that holonomy is a sufficient condition for the existence of a telescoper. But it is not a necessary condition (cf. Exercise 4 in Sect. 5.2). Nevertheless, show that $1/(nk+1)$, which is not holonomic according to Exercise 10 of Sect. 4.5, does not admit a telescoper.

22. Usually we apply Chyzak's algorithm to a module $M = C(x,t)[\partial_x,\partial_t]/I$, but the algorithm is not restricted to this case, and other choices are sometimes better. For example, for the integration of an algebraic function, we can take as M the function field to which the integrand belongs. Let $m = y^3 - (x+t)y + (t^2+x)$ and consider the algebraic function field $K = C(x,t)[y]/\langle m\rangle$. Compute a telescoper and a certificate for y

a. with $M = C(x,t)[D_x, D_t]/\operatorname{ann}(y)$;

b. with $M = K$.

23⋆. Just as proven in Theorem 5.40 for Zeilberger's algorithm, Chyzak's algorithm is guaranteed to find a minimal telescoper. Why does this not imply that the algorithm finds a minimal telescoper for a double sum/integral if we apply it twice? Illustrate this phenomenon with an example.

References

The term “creative telescoping” first appeared in van der Poorten’s account on Apéry’s proof that $\zeta(3)$ is irrational [439], where he reports that Zagier used the method to prove (by hand) one of the recurrences that appear in the proof. Zeilberger adopted the term “creative telescoping” in [469] for Algorithm 5.39. The algorithm itself was introduced in [467] as a “fast algorithm”, where the “fast” is meant in comparison to an earlier algorithm Zeilberger proposed in [468] which uses elimination techniques as discussed in Sect. 5.2 and is now sometimes called Zeilberger’s slow algorithm. The idea of certificates was introduced in a joint paper of Wilf and Zeilberger [457]. The same paper also introduces the idea of companion identities. Koornwinder studied the case of hypergeometric sums with non-natural boundaries [288] and gave a version of Zeilberger’s algorithm for the q-case [287].

Zeilberger’s algorithm has become a landmark in symbolic summation, which is covered in various textbooks [96, 223, 268, 283, 356].

The differential analog of creative telescoping has been known for centuries as method of differentiating under the integral sign. It was restricted to hand calculations until Almkvist and Zeilberger turned it into an algorithm for the case of hyperexponential integrands [30]. In order to highlight the close analogy between summation and integration, they developed Algorithm 5.5 as a differential analog of Gosper’s algorithm in the same paper. Some authors call Algorithm 5.5 the differential Gosper algorithm and refer to the creative telescoping method based on it as the Almkvist-Zeilberger algorithm.

Chyzak’s algorithm appears in [155] and is also nicely described in [153]. Koutschan’s algorithm is given in [290]. Wegschaider [453] already used linear algebra to find creative telescoping relations for hypergeometric multiple sums, but only searches for polynomial certificates and found that allowing denominators in the certificate does not work well. Koutschan comes to the opposite conclusion. The diverging observations are not surprising as the performance of the approach depends critically on a number of implementation details and on the nature of the problems to which it is applied.

There are further generalizations of creative telescoping. For example, Chen, Hou, and Jin [134] give a method that blends creative telescoping with summation by parts. Their algorithm can find recurrences for certain definite sums whose summand is the product of a hypergeometric term and some other quantity. Majewicz [318] gives an algorithm that handles sums involving terms like k^k, Kauers [261] gives an algorithm for sums involving Stirling numbers, and Chen and Sun give an algorithm for sums involving Bernoulli numbers or Euler numbers [132]. A common framework for all these generalizations was given by Chyzak, Kauers and Salvy [159]. Schneider [384] does creative telescoping in difference fields, using Karr’s summation algorithm in place of Gosper’s algorithm, and Raab [363] does creative telescoping in differential fields, using Risch’s integration algorithm in place of the Almkvist-Zeilberger algorithm.

5.5 Bounds

Koutschan's algorithm makes a guess for the common denominator of the certificate and increases its degree in each iteration. Once it arrives at a sufficiently large choice, it will detect a creative telescoping relation as a nonzero solution of a linear system. In order to derive a denominator size which is surely sufficient, we can once again apply the argument that a linear system with more variables than equations must have a nonzero solution. The analysis is particularly simple for bivariate rational functions in the differential case. The derivatives of a rational function $p/q \in C(x,t)$ with $\deg_x(p) < \deg_x(q) - 1$ have the form

$$D_t \cdot (\frac{p}{q}) = \frac{(D_t \cdot p)q - p(D_t \cdot q)}{q^2},$$

$$D_t^2 \cdot (\frac{p}{q}) = \frac{\boxed{\text{x-degree} \leq \deg_x(p) + 2\deg_x(q)}}{q^3},$$

$$\vdots$$

$$D_t^r \cdot (\frac{p}{q}) = \frac{\boxed{\text{x-degree} \leq \deg_x(p) + r\deg_x(q)}}{q^{r+1}},$$

where all we need to know about the numerators on the right hand sides is their degree in x. We do not claim that these numerators are coprime with q. Any $C(t)$-linear combination of the expressions above has the form

$$c_0(t)\frac{p}{q} + \cdots + c_r(t)D_t^r \cdot (\frac{p}{q}) = \frac{\boxed{x\text{-degree} \leq \deg_x(p) + r\deg_x(q)}}{q^{r+1}},$$

and the creative telescoping problem for $\frac{p}{q}$ is solved if we can write the right hand side as the x-derivative of a certain rational function. It is clear that a good choice for the denominator of such a rational function is q^r, and as the degree of the numerator of

$$D_x \cdot \frac{b_0(t) + \cdots + b_s(t)x^s}{q^r}$$
$$= \frac{(b_1(t) + \cdots + sb_s(t)x^{s-1})q - r(b_0(t) + \cdots + b_s(t)x^s)D_x \cdot q}{q^{r+1}}$$

is (at most) $s + \deg_x(q) - 1$, a good choice for the degree s of its numerator is $s = \deg_x(p) + r\deg_x(q) - (\deg_x(q) - 1) = \deg_x(p) + (r-1)\deg_x(q) + 1$.

For any specific choice of r, making an ansatz for a telescoper and a certificate with the shapes indicated above and equating the coefficients of the numerators leads to a linear system over $C(t)$ with $(r+1)+(s+1) = r+\deg_x(p)+(r-1)\deg_x(q)+3$

variables $c_0, \dots, c_r, b_0, \dots, b_s$ and $\deg_x(p) + r \deg_x(q) + 1$ equations. This system will have a solution if it has more variables than equations, and this will be the case for any $r \geq \deg_x(q) - 1$. Note that a nonzero solution of the linear system must give rise to a nonzero telescoper, because if we had a solution $(c_0, \dots, c_r, b_0, \dots, b_s)$ with $c_0 = \dots = c_r = 0$, then $D_x \cdot \frac{b_0(t)+\dots+b_s(t)x^s}{q^r}$ would be zero, which forces $b_0 = \dots = b_s = 0$. We have thus not only clarified the shape of the certificate, but we have also obtained an upper bound on the order of the minimal telescoper for the rational function $\frac{p}{q}$.

We can go a step further and also derive bounds on the degrees of the polynomials $c_0, \dots, c_r, b_0, \dots, b_s$. Such bounds can be obtained by doing a similar analysis as above. Let us determine a collection of pairs $(r, d) \in \mathbb{N}^2$ for which the rational function $\frac{p}{q}$ admits a telescoper of order $\leq r$ and degree $\leq d$. Applying a telescoper of the form $\sum_{i=0}^{r} \sum_{j=0}^{d} c_{i,j} t^j D_t^i$ to $\frac{p}{q}$ gives a rational function with denominator q^{r+1} and a numerator whose degree in x is at most $\deg_x(p) + r \deg_x(q)$ and whose degree in t is at most $d + \deg_t(p) + r \deg_t(q)$. The certificate needs to be a rational function whose x-derivative has the same shape, so its denominator should be q^r and its numerator should have x-degree at most $\deg_x(p) + (r-1)\deg_x(q) + 1$ and t-degree at most $d + \deg_t(p) + (r-1)\deg_t(q)$. Coefficient comparison will therefore lead to a linear system over C with

$$(r+1)(d+1) + (\deg_x(p) + (r-1)\deg_x(q) + 2)(d + \deg_t(p) + (r-1)\deg_t(q) + 1)$$

variables and

$$(\deg_x(p) + r \deg_x(q) + 1)(d + \deg_t(p) + r \deg_t(q) + 1)$$

equations. The number of variables exceeds the number of equations if r and d are as stated in the following result.

Theorem 5.51 *Let $p, q \in C[t, x]$.*

1. *If $\deg_x(p) < \deg_x(q) - 1$, let*

$$\alpha = \deg_x(q) - 2,$$
$$\beta = (2\deg_x(q) - 1)\deg_t(q) - 1,$$
$$\gamma = \deg_t(q)(\deg_x(p) - \deg_x(q) + 2) + \deg_t(p)(\deg_x(q) - 1) + \deg_x(q) - 2.$$

2. *If $\deg_x(p) \geq \deg_x(q) - 1$, let*

$$\alpha = \deg_x(q) - 1,$$
$$\beta = 2\deg_t(q)\deg_x(q) - 1,$$
$$\gamma = \deg_t(q)(\deg_x(p) - \deg_x(q) + 1) + (\deg_t(p) + 1)\deg_x(q) - 1.$$

Then for every $r, d \in \mathbb{N}$ with

$$r > \alpha \quad \text{and} \quad d > \frac{\beta r + \gamma}{r - \alpha}$$

there exists a telescoper $P \in C[t][D_t] \setminus \{0\}$ for $\frac{p}{q}$ of order r and degree d. □

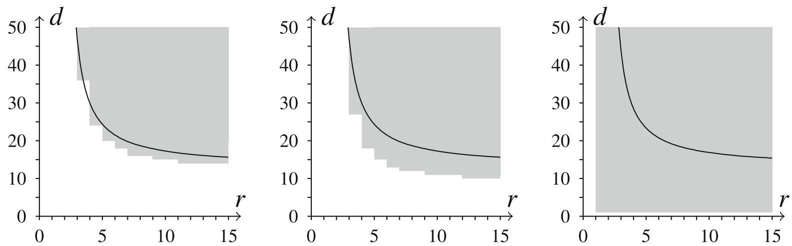
Proof The first case follows from the preceding discussion by checking that for the proposed restrictions on (r, d), the number of variables exceeds the number of equations in the linear system derived above. For the second case, see Exercise 1. ■

For rational functions p/q with squarefree denominator q, the bounds on the orders r are generically tight. The bounds on the degrees d are not tight. Slightly better bounds can be obtained by optimizing the shape of the ansatz for the telescoper, and Exercise 4 suggests one technique for doing so. Despite being suboptimal, the degree bounds do reflect the interesting phenomenon that telescopers of lower degrees can become available if we increase the order. This effect is not an artefact of the analysis but can also be observed if we look at the actual sizes of the telescopers for particular rational functions.

Example 5.52 In the figures below, we compare the degree bounds of Theorem 5.51 (curve) with the actual degrees of telescopers (shaded area) for the following three rational functions:

1. $\frac{-t^2x^2+t^2x+t^2-tx^2-tx+t+x^2+x-1}{t^2x^4-t^2x^3-t^2x^2+t^2x-t^2-tx^4+tx^3+tx^2+tx+t+x^4+x^3+x^2-x+1}$ (left)
2. $\frac{x^2-t^3}{x^4+t^2x^2+x+t+1}$ (middle)
3. $\frac{x^2-2t}{(x^2-t)(x^2-4t)}$ (right)

Note that the predicted degrees coincide for the first two rational functions, because their numerator and denominator degrees in x and t match. The actual degrees of their telescopers differ however. The third rational function has a telescoper of order 1 and degree 2 although the theorem only predicts a telescoper of order 3.



□

For other classes of integrands/summands, bounds on the orders and degrees of the telescopers can be derived in a similar way, and the typical result is a hyperbolic relationship like in the situation discussed above. We will only discuss one more case, the case of proper hypergeometric terms as defined in Definition 5.13, and as this case leads to rather messy calculations, we will only illustrate the argument by analyzing a very special instance. For nonnegative integers a, a', consider the hypergeometric term $h = \Gamma(an + a'k)$. Following Zeilberger's algorithm, we make an ansatz $P = c_0 + c_1 S_n + \cdots + c_s S_n^s$ for a telescoper and call Gosper's algorithm on $P \cdot h$. Gosper's algorithm in turn determines polynomials p, q, r such that

$$\frac{S_k P \cdot h}{P \cdot h} = \frac{\sigma_k(p)}{p} \frac{q}{\sigma_k(r)}.$$

For $h = \Gamma(an + a'k)$, we can take

$$p = \sum_{i=0}^{s} c_i (an + a'k)^{\overline{ia}}, \quad q = (an + a'k)^{\overline{a'}}, \quad r = 1,$$

where we use the notation $u^{\overline{\ell}} = u(u+1)\cdots(u+\ell-1)$ for polynomials u and integers $\ell \in \mathbb{N}$. The question is then whether the Gosper equation $p = q\sigma_k(y) - ry$ has a polynomial solution y. More precisely, for the purpose of deriving a bound on the order of the telescoper of h the question is for which values of s can we ensure that there is a solution. For any specific choice of s, we have $\deg_k(p) = sa$, and since $\max(\deg_k(r), \deg_k(q)) = a'$, a plausible target degree for y is $sa - a'$, so that the degree on both sides of the Gosper equation match. We then have $(s+1)+(sa-a'+1)$ variables and $sa+1$ equations, and therefore there must be a solution for every $s \geq a'$. This is the desired bound on the orders of the telescopers of h.

An analogous analysis can be carried out for hypergeometric terms of the form $\Gamma(an - a'k)$, $1/\Gamma(an + a'k)$, or $1/\Gamma(an - a'k)$ (Exercise 9), and with a sufficient amount of patience even for a general proper hypergeometric term. Moreover, it is possible to include the degree d of the telescoper in the analysis, by considering an ansatz over C rather than over $C(n)$. The resulting bounds are summarized in the following theorem.

Theorem 5.53 *For a proper hypergeometric term*

$$h = p(n,k)\phi^n \psi^k \prod_{m=1}^{M} \frac{\Gamma(a_m n + a'_m k + a''_m)\Gamma(b_m n - b'_m k + b''_m)}{\Gamma(u_m n + u'_m k + u''_m)\Gamma(v_m n - v'_m k + v''_m)}$$

with $p \in C[n,k]$, $\phi, \psi \in C$, $M \in \mathbb{N}$, $a_m, a'_m, b_m, b'_m, u_m, u'_m, v_m, v'_m \in \mathbb{N}$, $a''_m, b''_m, u''_m, v''_m \in C$, *let*

$$\vartheta = \max\Big\{\sum_{m=1}^{M}(a_m + b_m), \sum_{m=1}^{M}(u_m + v_m)\Big\}, \quad \delta = \text{total degree of } p \text{ in } n \text{ and } k,$$

$$\nu = \max\Big\{\sum_{m=1}^{M}(a'_m + v'_m), \sum_{m=1}^{M}(u'_m + b'_m)\Big\}, \quad \mu = \sum_{m=1}^{M}(a_m + b_m - u_m - v_m).$$

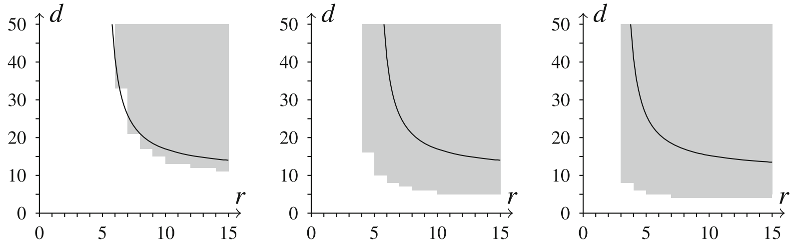
Suppose that h cannot be written as the product of a bivariate rational function and a univariate hypergeometric term in n. Then for every $(r, d) \in \mathbb{N}^2$ with

$$r \geq \nu \quad \text{and} \quad d \geq \frac{(\vartheta\nu - 1)r + \frac{1}{2}\nu(2\delta + |\mu| + 3 - (1 + |\mu|)\nu) - 1}{r - \nu + 1}$$

there exists a telescoper for h of order r and degree d. □

Example 5.54 In the figures below, we compare the degree bounds of Theorem 5.53 (curve) with the actual degrees of telescopers (shaded area) for the following three hypergeometric terms:

1. $\frac{\Gamma(2n+3k)}{\Gamma(n-3k)}$ is an example where the degree bound predicts the actual degrees quite accurately.
2. $\frac{\Gamma(2n-2k+1)\Gamma(n+k)}{\Gamma(2n+2k+1)\Gamma(n-3k)}$ is an example where the degree differences are more significant.
3. $\frac{\Gamma(n+1)^3}{\Gamma(k+1)^2\Gamma(2k+1)\Gamma(n-2k+1)\Gamma(n-k+1)^2}$ is an example where the order bound overshoots.



□

It follows from Theorems 5.51 and 5.53 that a telescoper of a rational function (in the differential case) or a hypergeometric term (in the shift case) can be computed in polynomial time. More precisely, in the first case the number of operations in C needed to compute a telescoper along with a certificate depends polynomially on the degrees of numerator and denominator in x and t. In the second case, the number of operations in C needed to compute a telescoper along with a certificate depends polynomially on the degrees of p in n and k as well as the integer parameters $a_m, a'_m, b_m, b'_m, u_m, u'_m, v_m, v'_m$. Note that these parameters do not measure the length of the input in the usual sense. In a strict sense, writing down a telescoper of a hypergeometric term may well consume exponentially more space than the hypergeometric term itself (Exercise 11).

Since telescopers of larger order can sometimes have lower degrees, we can trade order against degree. The arithmetic size of a telescoper of order r and degree d is $(r + 1)(d + 1)$, and if we assume for simplicity that the bounds given in Theorems 5.51 and 5.53 are tight, then it turns out that the smallest telescoper in terms of arithmetic size is not necessarily identical with the minimal telescoper. The optimal order can be easily computed by finding the minimum of $(r + 1)(f(r) + 1)$ where f denotes the function stated in Theorem 5.51 or in Theorem 5.53 as a bound on the degree. For example, in the differential case, the order which minimizes the arithmetic size of the telescoper turns out to be the integer closest to $\alpha + \sqrt{\frac{(\alpha+1)(\alpha\beta+\gamma)}{\beta+1}}$.

In the case $C = \mathbb{Q}$, the bitsize of a telescoper depends not only on its order and degree but also on the length of the integers appearing in its coefficients. The *height* of an operator in $\mathbb{Z}[x][\partial]$ is defined as the largest absolute value among the integer coefficients it contains. The bitsize of such an operator is then roughly the product of its order, its degree, and the logarithm of its height. A bound on the height of a telescoper can also be obtained by analyzing a linear algebra problem. For the bounds on order and degree derived above, we have set up a linear system with more variables than equations, so that it must have a solution. If we take a closer look at this linear system, we can bound the sizes of their entries, and from this information, and we can deduce a bound on the sizes of the coefficients of the solution vectors. These coefficients are precisely the integers appearing in the telescoper, so we can obtain the desired bound on their height in this way.

The calculations required to execute this approach are lengthy and tedious and not particularly interesting. We will therefore again only state the final outcome and discuss some special cases in the exercises (Exercise 16).

Theorem 5.55 *Let h be a proper hypergeometric term as in Theorem 5.53, now assuming in addition that the parameters $a''_m, b''_m, u''_m, v''_m$ appearing in it are integers. Let δ, ϑ, ν be as in Theorem 5.53 and let*

$$\Omega = \max_{m=1}^{M} \max\{a_m, a'_m, |a''_m|, b_m, b'_m, |b''_m|, u_m, u'_m, |u''_m|, v_m, v'_m, |v''_m|\}.$$

Then there exists a telescoper of h of order $r = \nu$ whose height is bounded by

$$\max\left\{|x|^\nu, |y|+1\right\} \|p\|_\infty^{\nu+1} (\delta+\vartheta\nu+1)!^{\nu+1} (\nu+1)^{\delta(\nu+1)} (|y|+1)^{\delta+(\vartheta-1)\nu+1}$$
$$\times\, \delta!^{2(\nu+1)} |x|^{\nu^2} (\delta+\vartheta\nu+1)^{\delta+(\vartheta+\delta+2)\nu+(\vartheta-1)\nu^2} (2(\nu+2)\Omega-2)^{(\delta+\vartheta+1)\nu+(2\vartheta-1)\nu^2},$$

where $\|p\|_\infty$ refers to the largest absolute value of the coefficients of p. □

The main motivation for computing telescopers of hypergeometric terms is to prove hypergeometric summation identities. The telescoper for the summand translates into a recurrence for the sum, and in order to prove that the sum is equal to a conjectured closed form, we check that the closed form satisfies the same recurrence and that a sufficient number of initial terms agree. The number of initial terms that need to be checked depends primarily on the order of the telescoper, but may be larger if the leading coefficient polynomial of the recurrence has integer roots (cf. Sect. 2.2). With the help of Theorems 5.53 and 5.55, we can tell in advance how large such an integer root can possibly be. We can then avoid the computation of a telescoper altogether and prove a hypergeometric summation identity as follows.

Algorithm 5.56 *(Yen's two-line algorithm)*
Input: *A hypergeometric term g in n and a proper hypergeometric term h in n and k such that the definite sum $\sum_k h$ has natural boundaries.*
Output: *True if $\sum_k h = g$, and false otherwise.*

1 *Determine a finite bound N such that the identity is true as soon as it is true for all $n \leq N$.*
2 *If the identity holds for $n = 0, \ldots, N$, then return true, otherwise return false.*

While the conceptual simplicity of this algorithm is attractive, the bounds N that we can obtain by inspection of the input are so high that the algorithm is far from having any practical relevance. Indeed, note that the height bound stated in Theorem 5.55 is exponential in the parameters, so the bound N obtained in step 1 will be exponential, too, and as step 2 compares N terms, we end up with an exponential runtime. On the other hand, it follows from the very same height bound of Theorem 5.55, in combination with the bounds on order and degree stated in Theorem 5.53, that there is a telescoper whose bitsize depends only polynomially on the parameters of the input term h, and computing this telescoper by linear algebra is also possible in polynomial time. It virtually never happens in practice that the leading coefficient polynomial of a telescoper has an extremely large integer root, so the preferred way for proving a hypergeometric summation identity is still to compute the telescoper explicitly.

Let us now turn from discussing degrees and heights of telescopers to bounds on their orders. As far as the minimal telescoper is concerned, Theorems 5.55 and 5.53 provide upper bounds on their orders (despite the "$r \geq \ldots$" appearing in the statement of Theorem 5.53). As we have seen, these upper bounds originate from sufficient conditions on the existence of telescopers. In order to derive lower bounds on the order of a minimal telescoper, we need a necessary condition for the existence of a telescoper. The defining property for a telescoper P for some f is that $P \cdot f$ is summable/integrable. For rational functions, we know from Theorem 5.2 that the only obstructions to being integrable are poles with nonzero residues. Residues with respect to x of a bivariate rational function $f \in C(t, x)$ are algebraic functions in t which are annihilated by the Rothstein-Trager resultant (part 3 of Theorem 5.4). We can say that the job of a telescoper for f is to annihilate these algebraic functions. More precisely: for an operator $P \in C(t)[D_t]\setminus\{0\}$ to be a telescoper of $f \in C(t, x)$, it is necessary and sufficient that it annihilates the residues of f.

This observation gives us more than just a bound on the order of the minimal telescoper. We can in fact use it as an alternative way for computing telescopers, as follows. First apply Hermite reduction to write f as $g' + h$, then compute the Rothstein-Trager resultant for h, and then call the algorithm behind part 3 of Theorem 3.29 to obtain an annihilating operator for the residues of h.

For hypergeometric terms, a similar reasoning gives us a lower bound on the order of the minimal telescoper. This requires a bit of preparation, which is interesting in its own right. We need to develop some kind of Hermite reduction for hypergeometric terms, which allows us to write a given hypergeometric term f in the form $(\Delta_k \cdot g) + h$ for some hypergeometric terms g and h with h minimal in some sense. Note that Gosper's algorithm does not qualify as such a reduction procedure because it only solves the problem if there is a solution with $h = 0$, and otherwise only asserts that there is no such solution but does not provide any further information. The following definition gives a meaning to h being minimal "in some sense." It uses the shell/kernel terminology introduced in Definition 2.72.

Definition 5.57 Let h be a hypergeometric term in k, let $s \in C(k)$ be a shell of h and $h_{\text{ker}} = h/s$ be the corresponding kernel. Let $u, v \in C[k]$ be such that $\sigma_k(h_{\text{ker}})/h_{\text{ker}} = u/v$. We say that h is *Abramov-Petkovšek reduced* (w.r.t. the decomposition $h = sh_{\text{ker}}$) if $s = \frac{a}{b} + \frac{c}{v}$ for certain $a, b, c \in C[k]$ with $\gcd(b, \sigma_k^{-i}(u)) = \gcd(b, \sigma_k^{i}(v)) = \gcd(b, \sigma_k^{i+1}(b)) = 1$ for all $i \in \mathbb{N}$. □

A key feature of an Abramov-Petkovšek reduced term is that such a term can be summable only if $b \mid a$.

Proposition 5.58 *In the notation of Definition 5.57, if h is Abramov-Petkovšek reduced and there is a hypergeometric term g such that $h = \Delta_k \cdot g$, then $b \mid a$.* □

Proof Let $w = \frac{p}{q} \in C(k)$ be such that $g = wh_{\text{ker}}$, so that $h = \Delta_k \cdot g$ translates into $\frac{a}{b} + \frac{c}{v} = \frac{u}{v}\sigma_k(w) - w$. Then $av + cb = bu\sigma_k(w) - bvw$. Since the left hand side is a polynomial, so must the right hand side be. We show that this forces q to be a constant.

Suppose otherwise and let q_0 be an irreducible factor of q. Let $i_{\max}, i_{\min} \in \mathbb{Z}$ be maximal and minimal, respectively, such that $\gcd(q, \sigma_k^{i_{\max}}(q_0)) \neq 1$ and $\gcd(q, \sigma_k^{i_{\min}}(q_0)) \neq 1$. Then $\sigma_k^{i_{\max}+1}(q_0)$ appears in the denominator of $\sigma_k(w)$ but not of w, and $\sigma_k^{i_{\min}}(q_0)$ appears in the denominator of w but not of $\sigma_k(w)$. Since the left hand side is a polynomial, we must have $\sigma_k^{i_{\max}+1}(q_0) \mid bu$ and $\sigma_k^{i_{\min}}(q_0) \mid bv$. Then $\gcd(bu, \sigma_k^{i_{\max}+1-i_{\min}}(bv)) \neq 1$. According to the condition in Definition 5.57, b has no common factors with $\sigma_k^{i_{\max}+1-i_{\min}}(v)$, nor with $\sigma_k^{-(i_{\max}+1-i_{\min})}(u)$, nor with $\sigma_k^{i_{\max}+1-i_{\min}}(b)$, so it follows that $\gcd(u, \sigma_k^{i_{\max}+1-i_{\min}}(v)) \neq 1$. This however is also not possible, because h is assumed to be a kernel.

This completes the argument that q is a constant. So w is a polynomial, and the right hand side of $av + cb = bu\sigma_k(w) - bvw$ is a polynomial which contains b as a divisor. Then $b \mid av + cb$, $b \mid av$, and finally $b \mid a$, using once more that $\gcd(b, v) = 1$. ■

Abramov-Petkovšek reduction takes as input an arbitrary hypergeometric term f and returns two hypergeometric terms g, h such that h is Abramov-Petkovšek reduced and $f = (\Delta_k \cdot g) + h$. The following algorithm starts with the hypothesis $h = f$ and successively moves portions of h into $\Delta_k \cdot g$ until the conditions of Definition 5.57 are met. It proceeds in three phases. In the first two phases, it writes h in the form $\frac{a}{b\sigma_k^{-1}(u)v} f_{\text{ker}}$ and eliminates factors of b that violate the requirements $\gcd(b, \sigma_k^{i}(v)) = 1$ and $\gcd(b, \sigma_k^{i+1}(b)) = 1$ for some $i \in \mathbb{N}$ (first phase) and the requirement $\gcd(b, \sigma_k^{-i}(u)) = 1$ for some $i \in \mathbb{N}$ (second phase). The third phase removes the factor $\sigma_k^{-1}(u)$ from the denominator of $\frac{a}{b\sigma_k^{-1}(u)v}$.

Algorithm 5.59 *(Abramov-Petkovšek reduction)*
Input: *A hypergeometric term f.*
Output: *Hypergeometric terms g, h such that h is Abramov-Petkovšek reduced and $f = (\Delta_k \cdot g) + h$.*

1 *Compute a shell $s \in C(k)$ of f, set $f_{\text{ker}} = f/s$, and let $u, v \in C[k]$ be such that $\frac{\sigma_k(f_{\text{ker}})}{f_{\text{ker}}} = \frac{u}{v}$.*
2 *Compute $a, b \in C[k]$ such that $s = \frac{a}{b\sigma_k^{-1}(u)v}$.*
3 *Set $w = 0$.*
4 *while $\exists\, i \in \mathbb{N} : \gcd(b, \sigma_k^i(v)) \neq 1$ or $\gcd(b, \sigma_k^{i+1}(b)) \neq 1$, do*
5 *Choose the largest such i and compute $g = \gcd(b, \operatorname{lcm}(\sigma_k^i(v), \sigma_k^{i+1}(b))) \in C[k]$.*
6 *If necessary, increase the multiplicities of the irreducible factors of g so that $\gcd(b\sigma_k^{-1}(u)v/g, g) = 1$ (cf. Exercise 19).*
7 *Determine $p, q \in C[k]$ such that $s = \frac{p}{b\sigma_k^{-1}(u)v/g} + \frac{q}{g}$.*
8 *Replace s by $s - \frac{q}{g} + \sigma_k^{-1}(\frac{vq}{ug})$ and w by $w + \sigma_k^{-1}(\frac{vq}{ug})$. Recompute a, b as in line 2 for the new s.*
9 *while $\exists\, i \in \mathbb{N} : \gcd(b, \sigma_k^{-i}(u)) \neq 1$, do*
10 *Choose the largest such i and construct a $g = \gcd(b, \sigma_k^{-i}(u)) \in C[k]$.*
11 *If necessary, increase the multiplicities of the irreducible factors of g so that $\gcd(b\sigma_k^{-1}(u)v/g, g) = 1$ (cf. Exercise 19).*
12 *Determine $p, q \in C[k]$ such that $s = \frac{p}{b\sigma_k^{-1}(u)v/g} + \frac{q}{g}$.*
13 *Replace s by $s + \frac{u}{v}\sigma_k(\frac{q}{g}) - \frac{q}{g}$ and w by $w - \frac{q}{g}$. Recompute a, b as in line 2 for the new s.*
14 *Compute $p_1, p_2, p_3 \in C[k]$ such that $s = \frac{p_1}{b} + \frac{p_2}{\sigma_k^{-1}(u)} + \frac{p_3}{v}$.*
15 *Replace s by $s + \frac{\sigma_k(p_2)}{v} - \frac{p_2}{\sigma_k^{-1}(u)}$ and w by $w - \frac{p_2}{\sigma_k^{-1}(u)}$.*
16 *Return $g = wf_{\text{ker}}$ and $h = sf_{\text{ker}}$.*

Theorem 5.60 *Algorithm 5.59 is correct and terminates.* □

Proof For the correctness, observe first that the updates in lines 8 and 13 are such that $\frac{u}{v}\sigma_k(w) - w + s$ remains fixed throughout the two loops; the adjustments of s are compensated by the adjustments of w. The same is true for the final adjustment in line 15. Therefore, in view of $\Delta_k \cdot wf_{\text{ker}} = (\frac{u}{v}\sigma_k(w) - w)f_{\text{ker}}$, we have $f = (\Delta_k \cdot g) + h$ for the terms g and h defined in line 16.

It remains to show that h is Abramov-Petkovšek reduced. Two of the three required properties of b are arranged in the first loop (if it terminates), and the third is arranged in the second loop (if it terminates). We only need to check that the second loop does not destroy the properties arranged by the first loop. To see that this cannot happen, observe that any new irreducible factor that may enter b in line 13 is contained in $\sigma_k(g)$. By the choice of g, any such factor is contained in $\sigma_k^{-i+1}(u)$ and can therefore not also be contained in $\sigma_k^j(v)$ for any $j \in \mathbb{N}$, because f_{ker} is a kernel. Moreover, a factor of $\sigma_k(g)$ cannot be contained in $\sigma_k^{j+1}(b)$ for any $j \in \mathbb{N}$, because i is chosen maximally in line 5.

For the termination, consider the first loop. The argument for the second loop is similar. We show that in each iteration the value of i is strictly smaller than in the previous iteration. Consider the value of i in a certain iteration and write $b_{\mathrm{old}}, b_{\mathrm{new}}$ for the values of b at the beginning and at the end of this iteration, respectively. In line 8, b_{new} is obtained from b_{old} by removing all factors of g at the cost of possibly introducing some factors of $\sigma_k^{-1}(ug)$. Factors of g cannot also appear in $\sigma_k^{-1}(g)$, because if r were a nontrivial irreducible factor of both g and $\sigma_k^{-1}(g)$, then it would be a common factor of $\sigma_k^{-1}(b_{\mathrm{old}})$ and $\operatorname{lcm}(\sigma_k^i(v), \sigma_k^{i+1}(b_{\mathrm{old}}))$, so $\gcd(b_{\mathrm{old}}, \operatorname{lcm}(\sigma_k^{i+1}(v), \sigma_k^{i+2}(b_{\mathrm{old}}))) \neq 1$, in contradiction to the maximality of i. Therefore, none of the factors of g which get removed from b_{old} can get reintroduced by $\sigma_k^{-1}(g)$.

It is also not possible that there is a $j \geq i$ such that

$$\gcd(b_{\mathrm{new}}, \operatorname{lcm}(\sigma_k^j(v), \sigma_k^{j+1}(b_{\mathrm{new}}))) \neq 1.$$

To see this, consider an irreducible factor r of b_{new}. Then r is contained either in b_{old} or in $\sigma_k^{-1}(g)$. If it is contained in b_{old}, it cannot be contained in $\operatorname{lcm}(\sigma_k^j(v), \sigma_k^{j+1}(b_{\mathrm{new}}))$, by the maximality of i and the definition of b_{new}. So suppose that r is contained in $\sigma_k^{-1}(g)$. It then appears in $\sigma_k^{-1}(b_{\mathrm{old}})$ but not in $\sigma_k^j(g)$ (because $\sigma_k^{-1}(g)$ and $\sigma_k^j(g)$ are coprime by the maximality of i), so if it is also a factor of $\operatorname{lcm}(\sigma_k^j(v), \sigma_k^{j+1}(b_{\mathrm{new}}))$, then it is in fact a common factor of $\sigma_k^{-1}(b_{\mathrm{old}})$ and $\operatorname{lcm}(\sigma_k^j(v), \sigma_k^{j+1}(b_{\mathrm{old}}))$, which implies $\gcd(b_{\mathrm{old}}, \operatorname{lcm}(\sigma_k^{j+1}(v), \sigma_k^{j+2}(b_{\mathrm{old}}))) \neq 1$, again in contradiction to the maximality of i. ■

Example 5.61 Consider the hypergeometric term $f = \frac{k^4+5k^3-k^2-5k-2}{k^2(k+1)^3(k+2)}\binom{2k}{k}$. We can take $s = \frac{k^4+5k^3-k^2-5k-2}{k^2(k+1)^3(k+2)}$ as its shell and have $f_{\mathrm{ker}} = \binom{2k}{k}$ as the kernel. Then $\frac{u}{v} = \frac{2(2k+1)}{k+1}$. At the beginning, we have $b = k^2(k+1)^2(k+2)$.

Entering into the first loop, we find $i = 1$ and set $g = k + 2$. In line 6 we get the decomposition $s = -\frac{5k^4+4k^3+2k^2+2k+1}{k^2(k+1)^3} + \frac{5}{k+2}$, so we update s to

$$s - \frac{2(2k+1)}{k+1}\,\frac{k+1}{2(2k+1)}\,\frac{5}{k+2} + \frac{k}{2(2k-1)}\,\frac{5}{k+1} = -\frac{15k^5 - 4k^4 - 5k^3 + 4k^2 - 2}{2k^2(k+1)^3(2k-1)}$$

and set $w = \frac{5k}{2(2k-1)(k+1)}$ in line 7.

In the next iteration we have $b = k^2(k+1)^2$ and find $i = 0$, which gives $g = (k+1)^3$. Note that $\gcd(b, \sigma_k(b)) = (k+1)^2$ but we have to raise the exponent of

$k+1$ in g to 3 in order to enforce $\gcd(b\sigma_k^{-1}(u)v/g, g) = 1$. The decomposition in line 6 is then $s = \frac{17k^2-18k+6}{6k^2(2k-1)} - \frac{31k^2+26k+7}{6(k+1)^3}$, which leads us to update s to

$$s+\frac{2(2k+1)}{k+1}\frac{k+1}{2(2k+1)}\frac{31k^2+26k+7}{6(k+1)^3}-\frac{k}{2(2k-1)}\frac{31k^2-36k+12}{6k^3} = \frac{1}{4(2k-1)}$$

and to update w to $w - \frac{k}{2(2k-1)}\frac{31k^2-36k+12}{6k^3} = -\frac{k^3-5k^2-24k+12}{12k^2(2k-1)(k+1)}$.

Now we have $b = k^2$ and the first loop terminates. There is no work to do for the second loop. In line 12, we have $p_1 = p_3 = 0$ and $p_2 = 1/2$, so we update s to

$$s + \frac{1}{2(k+1)} - \frac{1}{4(2k-1)} = \frac{1}{2(k+1)}$$

and w to $w - \frac{1}{4(2k-1)} = -\frac{k^2-6}{6k^2(k+1)}$ in line 13.

The final result $f = \Delta_k \cdot (wf_{\mathrm{ker}}) + sf_{\mathrm{ker}}$ can be interpreted as the simplification

$$\sum_{k=1}^{n-1}\frac{k^4+5k^3-k^2-5k-2}{k^2(k+1)^3(k+2)}\binom{2k}{k} = -\frac{n^2-6}{6n^2(n+1)}\binom{2n}{n}+\frac{5}{6}+\sum_{k=1}^{n-1}\frac{1}{2(k+1)}\binom{2k}{k}.$$

We have split the complicated sum on the left into a closed form and a more simple sum. □

Equipped with Abramov-Petkovšek reduction, we can return to the task of bounding the order of the minimal telescoper of a bivariate hypergeometric term from below. We consider a hypergeometric term f in two variables n and k and view it as a hypergeometric term in k over the field $C(n)$. We want to exploit the necessary condition of Proposition 5.58. First we apply the Abramov-Petkovšek reduction to f, obtaining g, h such that $f = (\Delta_k \cdot g) + h$ where h is Abramov-Petkovšek reduced. Note that $P \in C(n)[S_n]$ is a telescoper for f if and only if it is a telescoper for h, because the part $(\Delta_k \cdot g)$ can be absorbed into the certificate. Next, write $h = (\frac{a}{b} + \frac{c}{v})h_{\mathrm{ker}}$ as in Definition 5.57. If $b \nmid a$ in $C(n)[k]$, we know from Proposition 5.58 that h is not summable. Since $P \cdot h$ must be summable in order for P to be a telescoper, it follows that $\operatorname{ord}(P) \geq 1$ in this case, because $\operatorname{ord}(P) = 0$ would mean that P is just an element of $C(n)$, and multiplying h by such an element won't suffice to change anything about $b \nmid a$.

The following theorem is a generalization of this reasoning. Its proof is based on analyzing how far the order of an operator $P \in C(n)[S_n]$ can be raised before $P \cdot h$ has a chance to meet the necessary condition of Proposition 5.58.

Theorem 5.62 *Let h be a hypergeometric term in n and k. Let $s \in C(n,k)$ be a shell of h w.r.t. k and let $h_{\mathrm{ker}} = h/s$ be the corresponding kernel. Let $u, v \in C(n)[k]$ be such that $\sigma_k(h_{\mathrm{ker}})/h_{\mathrm{ker}} = u/v$. Suppose that h is Abramov-Petkovšek reduced w.r.t. k, and let $a, b, c \in C(n)[k]$ be such that $s = \frac{a}{b} + \frac{c}{v}$ and*

$\gcd(a, b) = \gcd(b, \sigma_k^{-i}(u)) = \gcd(b, \sigma_k^i(v)) = \gcd(b, \sigma_k^{i+1}(b)) = 1$ *for all* $i \in \mathbb{N}$. *Let* $d \in C(n)[k]$ *be the denominator of* $\sigma_n(h_{\mathrm{ker}}/v)/(h_{\mathrm{ker}}/v)$. *Let* $P \in C(n)[S_n]$ *be a telescoper for* h. *Then for every irreducible factor* $p \in C(n)[k]$ *of* b *we have*

$$\operatorname{ord}(P) \geq \min\{r \in \mathbb{N} \setminus \{0\} : \exists\, \ell \in \mathbb{Z} : \sigma_k^\ell(p) \mid \sigma_n^r(b)\sigma_n^{r-1}(d)\}.$$

□

Proof Write the telescoper as $P = p_0 + \cdots + p_r S_n^r$. We may assume that $p_0 \neq 0$, because otherwise we can replace P by $p_1 + p_2 S_n + \cdots + p_r S_n^{r-1}$, which is then also a telescoper.

Writing $e \in C(n)[k]$ for the numerator of $\sigma_n(h_{\mathrm{ker}}/v)/(h_{\mathrm{ker}}/v)$, we have

$$\begin{aligned} S_n^i \cdot h = S_n^i \cdot \Big(\frac{a}{b} + \frac{c}{v}\Big) h_{\mathrm{ker}} &= S_n^i \cdot \Big(\frac{av}{b} + c\Big)\frac{h_{\mathrm{ker}}}{v} \\ &= \Big(\frac{\sigma_n^i(av)}{\sigma_n^i(b)} + \sigma_n^i(c)\Big)\frac{e\sigma_n(e)\cdots\sigma_n^{i-1}(e)}{d\sigma_n(d)\cdots\sigma_n^{i-1}(d)}\frac{h_{\mathrm{ker}}}{v}, \end{aligned}$$

for every $i \in \mathbb{N}$, and therefore

$$P \cdot h = \sum_{i=0}^{r} p_i \Big(\frac{\sigma_n^i(av)}{\sigma_n^i(b)} + \sigma_n^i(c)\Big)\frac{e\sigma_n(e)\cdots\sigma_n^{i-1}(e)}{d\sigma_n(d)\cdots\sigma_n^{i-1}(d)}\frac{h_{\mathrm{ker}}}{v}.$$

Since h_{ker} is a kernel, so is h_{ker}/v, and if $(\frac{a}{b} + \frac{c}{v})h_{\mathrm{ker}}$ is Abramov-Petkovšek reduced w.r.t. the kernel h_{ker}, then $(\frac{av}{b} + c)\frac{h_{\mathrm{ker}}}{v}$ is Abramov-Petkovšek reduced w.r.t. the kernel h_{ker}/v (Exercise 23).

With respect to the kernel h_{ker}/v, the shell of $P \cdot h$ is $\sum_{i=0}^r p_i(\sigma_n^i(\frac{a}{v})b + \sigma_n^i(c))\prod_{j=0}^{i-1}\sigma_n^j(\frac{e}{d})$. Since $P \cdot h$ is summable because P is a telescoper, Proposition 5.58 enforces that $P \cdot h$ is either not Abramov-Petkovšek reduced or that it is a polynomial.

Consider an irreducible factor $p \in C(n)[k]$ of b. Because of $\gcd(a, b) = \gcd(v, b) = 1$ and $p_0 \neq 0$, the summand $p_0\frac{av}{b}$ contains p in its denominator. If the shell is a polynomial, the factor p must appear again in the denominator of one of the other terms in order to enable cancellation. This requires $p \mid \sigma_n^i(b)\prod_{j=0}^{i-1}\sigma_n^{j-1}(d)$ for some $i \in \{0, \ldots, r\}$. If the shell is not a polynomial, then $P \cdot h$ cannot be Abramov-Petkovšek reduced, because it is summable. Applying Abramov-Petkovšek reduction to $P \cdot h$ can only eliminate the factor p from the denominator of the shell if there is some $\ell \in \mathbb{Z} \setminus \{0\}$ such that also $\sigma_k^\ell(p)$ appears in the denominator of the shell. This is only possible if $\sigma_k^\ell(p) \mid \sigma_n^i(b)\prod_{j=0}^{i-1}\sigma_n^{j-1}(d)$ for some $i \in \{0, \ldots, r\}$.

We have thus shown that for every irreducible factor $p \in C(n)[k]$ of b, there must be an $\ell \in \mathbb{Z}$ so that $\sigma_k^\ell(p) \mid \sigma_n^i(b)\prod_{j=0}^{i-1}\sigma_n^{j-1}(d)$ for some $i \in \{0, \ldots, r\}$. This is the case if and only if $\sigma_k^\ell(p) \mid \sigma_n^i(b)\sigma_n^{i-1}(d)$ for some $i \in \{0, \ldots, r\}$. The bound on $\operatorname{ord}(P)$ stated in the theorem follows from here. ■

We have shown in Theorem 5.14 that every proper hypergeometric term admits a telescoper by exploiting that shifting a polynomial $an + a'k$ in n by a' has the same effect as shifting it in k by a. The application of Theorem 5.62 is based on similar considerations.

Example 5.63 For the term $h = (\frac{1}{(4n+k)(n+3k)} + \frac{1}{(k+1)})\binom{n+k}{k}$ we can take $h_{\text{ker}} = \binom{n+k}{k}$ and set $u = k + n + 1$, $v = k + 1$, $a = c = 1$, $b = (4n + k)(n + 3k)$. We have $\sigma_n(h_{\text{ker}}/v)/(h_{\text{ker}}/v) = (k + n + 1)/(n + 1)$, so we can take $d = n + 1$. As d does not involve k, it plays no role in this example. For any $r \in \mathbb{N}$ we have $\sigma_n^r(b) = (4n + k + 4r)(n + 3k + r)$.

For the factor $p = 4n + k$ of b and any $\ell \in \mathbb{Z}$, we have $\sigma_k^\ell(p) = 4n + k + \ell$. This factor overlaps with the factor $4n + k + 4r$ of $\sigma_n^r(b)$ if $\ell = 4r$, and as such an ℓ can be found for every choice of $r \in \mathbb{N} \setminus \{0\}$, the factor p only implies that the order of any telescoper of h is at least 1.

For the factor $p = n + 3k$ of b and any $\ell \in \mathbb{Z}$ we have $\sigma_k^\ell(p) = n + 3k + 3\ell$. This factor overlaps with the factor $n + 3k + r$ of $\sigma_n^r(b)$ if $3\ell = r$. Such an ℓ exists if and only if $3 \mid r$, and the smallest $r \in \mathbb{N} \setminus \{0\}$ is 3. Therefore, this factor implies that the order of any telescoper of h is at least 3.

The actual order of the minimal telescoper of h turns out to be 4. □

Not all polynomials have the feature that shifts in n of suitable length can be compensated by shifts in k of suitable lengths. For example, for $p = nk + 1$ we have $\sigma_k^\ell(p) = nk + n\ell + 1$ and $\sigma_n^r(p) = nk + kr + 1$ for all $\ell, r \in \mathbb{Z}$, and these two polynomials, viewed as elements of $C(n)[k]$, overlap only if $\ell = r = 0$. For a proper hypergeometric term, there is no chance that we will encounter a b which contains $p = nk + 1$ as a factor. For such terms, b can only be a product of integer-linear polynomials. Note however that Theorem 5.62 is not restricted to proper hypergeometric terms. If it is applied to a term h for which b contains irreducible factors that are not integer-linear, it can happen that the lower bound predicted by the theorem is infinity. In this case, h does not have a telescoper.

Example 5.64 Consider $h = \frac{1}{nk+1}\binom{n}{k}$. We can write $h = (\frac{a}{b} + \frac{c}{v})h_{\text{ker}}$ with $a = 1$, $b = nk + 1$, $c = 0$, $v = k + 1$, $h_{\text{ker}} = \binom{n}{k}$. We have $\sigma_n(h_{\text{ker}}/v)/(h_{\text{ker}}/v) = (n + 1)/(n - k + 1)$, so we can take $d = n - k + 1$. Consider the factor $p = nk + 1$ of b. As there is no positive integer r such that $\sigma_k^\ell(p) \mid \sigma_n^r(b)\sigma_n^{r-1}(d)$, Theorem 5.62 asserts that the order of the minimal telescoper is at least infinity. In other words, h does not have a telescoper. □

We conclude this section with an example where we derive a lower bound on the order of the minimal telescoper without resorting to Theorem 5.62. Instead, the argument will be similar to the approach we used at the beginning of the section for deriving upper bounds. We will follow the execution of Zeilberger's algorithm and inspect the Gosper equation for an undetermined candidate of order r and then determine the smallest r for which this equation can possibly have a polynomial solution. The example also serves as a reminder that the minimal telescoper of a hypergeometric term (with natural boundaries) need not be the minimal annihilating operator of the definite sum over this term, although in most other examples it is.

Example 5.65 For a fixed integer $\alpha \geq 2$, consider the bivariate hypergeometric term $f_\alpha(n,k) := (-1)^k \binom{n}{k}\binom{\alpha k}{n}$. It can be shown (Exercise 25) that the definite sum $\sum_k f_\alpha(n,k)$ evaluates to $(-\alpha)^n$ and is therefore annihilated by the first order operator $S_n + \alpha$. We shall show that the minimal telescoper of $f_\alpha(n,k)$ has at least order α.

Let us see what happens if we apply Zeilberger's algorithm to $f_\alpha(n,k)$. Using

$$\frac{f_\alpha(n+i,k)}{f_\alpha(n,k)} = (-1)^i \frac{(-\alpha k+n)^{\overline{i}}}{(-k+n+1)^{\overline{i}}} \quad (i \in \mathbb{N})$$

we find that the application of a telescoper candidate $P = p_0 + p_1 S_n + \cdots + p_r S_n^r$ to $f_\alpha(n,k)$ yields

$$\begin{aligned} P \cdot f_\alpha(n,k) &= \sum_{i=0}^{r} p_i (-1)^i \frac{(-\alpha k+n)^{\overline{i}}}{(-k+n+1)^{\overline{i}}} f_\alpha(n,k) \\ &= \sum_{i=0}^{r} p_i (-1)^i (-\alpha k+n)^{\overline{i}} (-k+n+1+i)^{\overline{r-i}} \frac{f_\alpha(n,k)}{(-k+n+1)^{\overline{r}}}. \end{aligned}$$

For the hypergeometric term $\tilde{f}_\alpha(n,k) := \frac{f_\alpha(n,k)}{(-k+n+1)^{\overline{r}}}$, we have

$$\frac{\tilde{f}_\alpha(n,k+1)}{\tilde{f}_\alpha(n,k)} = \frac{(k-n-r)(\alpha k+1)^{\overline{\alpha}}}{(k+1)(\alpha k+1-n)^{\overline{\alpha}}}.$$

Note that no shift in k of the denominator by a positive integer gives a polynomial that has a common factor with the numerator. Therefore, the Gosper equation is

$$\begin{aligned} &\sum_{i=0}^{r} p_i (-1)^i (-\alpha k+n)^{\overline{i}} (-k+n+1+i)^{\overline{r-i}} \\ &= (k-n-r)(\alpha k+1)^{\overline{\alpha}} \sigma_k(y) - k(\alpha k+1-n-\alpha)^{\overline{\alpha}} y, \qquad \text{(G)} \end{aligned}$$

for unknown parameters $p_0, \ldots, p_r \in C(n)$ and an unknown polynomial $y \in C(n)[k]$.

Under which circumstances can this equation have a nontrivial solution? The left hand side is a polynomial in k of degree at most r, and the right hand side must match this degree. Naively, if y has degree d, we might expect the right hand side to have degree $\alpha + d + 1$, but the degree can be lower if some terms cancel. In order to understand which cancellations can occur, write

$$(k-n-r)(\alpha k+1)^{\overline{\alpha}} = \alpha^\alpha k^{\alpha+1} + \tfrac{1}{2}(\alpha+1-2n-2r)\alpha^\alpha k^\alpha + \cdots,$$
$$k(\alpha k+1-n-\alpha)^{\overline{\alpha}} = \alpha^\alpha k^{\alpha+1} - \tfrac{1}{2}(2n+\alpha-1)\alpha^\alpha k^\alpha + \cdots.$$

We see that the coefficient of $k^{\alpha+1+d}$ on the right hand side of (G) is $\alpha^\alpha \operatorname{lc}_k(\sigma_k(y)) - \alpha^\alpha \operatorname{lc}_k(y) = 0$, so the terms of highest degree cancel. For the next coefficient, rephrase the right hand side of (G) into

$$\begin{aligned}&(k-n-r)(\alpha k+1)^{\overline{\alpha}}\Delta_k(y) - (k(\alpha k+1-n-\alpha)^{\overline{\alpha}} - (k-n-r)(\alpha k+1)^{\overline{\alpha}})y\\ &= \alpha^\alpha k^{\alpha+1} d \operatorname{lc}_k(y) k^{d-1} - (r-\alpha)\alpha^\alpha k^\alpha \operatorname{lc}_k(y) k^d + \text{lower order terms.}\end{aligned}$$

The coefficient of $k^{\alpha+d}$ on the right hand side of (G) is thus $(d-(r-\alpha))\alpha^\alpha \operatorname{lc}_k(y)$. If this coefficient is zero as well, then $d = r-\alpha$, and since $d = \deg_y(y)$ is nonnegative, this implies $r \geq \alpha$. If the coefficient is not zero, then the degree of the right hand side of (G) is equal to $d+\alpha$, and since it must match the degree of the left hand side of (G), which is at most r, it follows again that $r \geq \alpha$.

We have thus shown that the order of any telescoper P for $f_\alpha(n,k)$ must be at least α. □

Exercises

1*.** Where did we use the assumption $\deg_x(p) < \deg_x(q)-1$ in the introductory discussion? Check the formulas given in part 2 of Theorem 5.51 for the case $\deg_x(p) \geq \deg_x(q) - 1$.

2. In the derivation of Theorem 5.51 we chose the degree $s = \deg_x(p) + (r-1)\deg_x(q) + 1$ for the numerator of the certificate. How does the resulting bound on r change if we use instead a larger degree $s+n$, for some $n \in \mathbb{N}$?

3*. According to Theorem 5.51, every rational function $\frac{p}{q} \in C(x,t)$ with $\deg_x(p) < \deg_x(q) - 1$ admits a telescoper of order at most $\deg_x(q) - 1$. Show that this bound can be improved to $\deg_x(q^*) - 1$, where q^* is the squarefree part of q in $C(t)[x]$.

4*. In the interest of simplicity, we have used a rectangular support in the ansatz for the telescoper in the derivation of Theorem 5.51. A slightly better degree estimate can be obtained by an ansatz of a more carefully chosen shape. The idea is similar to Verbaeten completion (cf. Exercise 16 in Sect. 5.2) and exploits the fact that $\deg_t(q^{r+1} D_t^i \cdot \frac{p}{q}) \leq \deg_t(p) + r\deg_t(q) - i$. For a certain $w \leq \min(r +$

$1, d+1)$ consider an ansatz for the telescoper of the form $\sum_{i=0}^{w-1}\sum_{j=0}^{d-w+i} c_{i,j}t^j D_t^i + \sum_{i=w}^{r}\sum_{j=0}^{d} c_{i,j}t^j D_t^i$. Assume for simplicity that $\deg_x(p) < \deg_x(q) - 1$.

a. What is the number of variables in this ansatz?

b. What is the resulting number of equations?

c. Which ansatz for the certificate (with rectangular support) fits well in this setup?

d. Derive a degree bound for the telescoper depending on the parameter w.

e. Which choice of w leads to the best bound?

5. For a pair $(r, d) \in \mathbb{N}^2$ satisfying the inequalities stated in Theorem 5.51 we get a telescoper of arithmetic size $(r+1)(d+1)$. What is the arithmetic size of the corresponding certificate?

6*. Produce pictures like in Example 5.54 for the following hypergeometric terms:

a. $\frac{\Gamma(2n-2k)}{\Gamma(n+4k)}$

b. $\frac{\Gamma(n+k)\Gamma(n-k)}{\Gamma(2n+2k+1)\Gamma(3n-3k+1)}$

c. $\frac{\Gamma(n+k)\Gamma(n-k)}{\Gamma(2n+2k+1)\Gamma(3n-3k)}$

7*. The hypergeometric term $(-1)^k\binom{n}{k}\binom{4n+k}{2n}$ has a telescoper of order 1 and degree 3. Show that it does not have a telescoper of higher order and lower degree.

8*. Let h be a hypergeometric term.

a. Let $r_{\min}$ be minimal such that h has a telescoper of order $r_{\min}$, and let $d_{\min}$ be minimal such that h has a telescoper of order $r_{\min}$ and degree $d_{\min}$. Show that this telescoper of order $r_{\min}$ and degree $d_{\min}$ is unique up to multiplication by constants.

b. Let now $r \geq r_{\min}$ be arbitrary, and let d be minimal such that h has a telescoper of order r and degree d. Is such a telescoper of order r and degree d also unique up to multiplication by constants?

9. For $b, b', u, u', v, v' \in \mathbb{N}$ and $P = c_0 + c_1 S_n + \cdots + c_s S_n^s$, determine p, q, r such that $\frac{S_k P \cdot h}{P \cdot h} = \frac{\sigma_k(p)}{p}\frac{q}{\sigma_k(r)}$, where **a.** $h = \Gamma(bn - b'k)$; **b.** $h = 1/\Gamma(un + u'k)$; **c.** $h = 1/\Gamma(vn - v'k)$.

10*. In the derivation of Theorem 5.53, we wrote $\frac{S_k P \cdot h}{P \cdot h}$ as $\frac{\sigma_k(p)}{p}\frac{q}{\sigma_k(r)}$ for certain polynomials p, q, r. This was motivated by the Gosper form, but for a Gosper form we need the additional condition $\gcd(q, \sigma_k^i(r)) = 1$ for all $i \in \mathbb{N} \setminus \{0\}$. In general, this condition is not satisfied for the p, q, r given in the text and in Exercise 9. Why is this not a problem?

11*. Construct a family of proper hypergeometric terms f_α $(\alpha \in \mathbb{N})$ such that the bitsize of f_α grows at most logarithmically in α while the arithmetic size of the minimal telescoper (understood as the product of its order and degree) grows at least polynomially in α.

12. Show that the bound given in Theorem 5.53 on the order of the minimal telescoper of a proper hypergeometric term can overshoot arbitrarily far. More precisely, show that for every $r \in \mathbb{N}$ there is a proper hypergeometric term which has a telescoper of order 0 but for which Theorem 5.53 only predicts the existence of telescopers of order $\geq r$.

13. Show that for every n there is a rational function $\frac{p}{q} \in C(x,t)$ with a squarefree denominator $q \in C(t)[x]$ of degree n in x which admits a telescoper of order 1.

14. Suppose that for certain $\alpha, \beta, \gamma \geq 0$, a certain summand/integrand admits a telescoper of order r and degree d for every (r,d) with $r \geq \alpha$ and $d \geq \frac{\beta r+\gamma}{r-\alpha+1}$, and assume that these bounds are tight. Determine the point (r,d) for which $r+d$ is minimal.

15****.** Let $p, q \in \mathbb{Z}[x,t]$ be polynomials with coefficients whose absolute values are bounded by some $M \in \mathbb{N}$. Assume that $\deg_x(p) < \deg_x(q) - 1$.

a. For $r \in \mathbb{N}$ and $i \in \{0,\dots,r\}$, show that the coefficients of the polynomial $q^{r+1} D_t^i \cdot \frac{p}{q} \in \mathbb{Z}[x,t]$ are bounded by $M^{r+1}(\deg_t(p) + r\deg_t(q))^r$.

b. Derive a bound on the integers appearing in a telescoper for $\frac{p}{q}$ of order r and degree d, for a choice of r and d satisfying the inequalities in Theorem 5.51.

16. Let $a, a', i \in \mathbb{N}$ and $a'' \in \mathbb{Z}$, and let $\Omega \in \mathbb{N}$ be such that $\Omega \geq \max\{a, a', |a''|\}$. Show that $||(an + a'k + a'')^{\overline{ia}}||_\infty \leq \Omega^{\overline{ia}}$.

17. Let $p \in \mathbb{Z}[x]$ and let $\xi \in \mathbb{Z}$ be a root of p. Show that $|\xi| \leq \|p\|_\infty$.

18. Consider a differential operator $P \in \mathbb{Z}[x][D]$ of order r and degree d whose integer coefficients are bounded in absolute value by M. Let $a = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}[[x]]$ be such that $P \cdot a = 0$ and $a_n = 0$ for $n = 0, \dots, 1 + 2Mr!$. Show that $a = 0$.

19. For $p, q \in C[x]$ monic with $p \mid q$, show that there is a $g \in C[x]$ such that $g^* \mid p \mid g \mid q$ and $\gcd(g, q/g) = 1$, where g^* is denotes the squarefree part of g. Propose an algorithm for finding such a g given p and q.

20****.** Show that the second loop in Algorithm 5.59 terminates.

21***.** Apply the Abramov-Petkovšek reduction to $\frac{2k(3k+2)}{(2k+1)(2k+3)(k+1)}\binom{2k}{k}$.

22****.** Here is a differential version of Proposition 5.58: Let h be a hyperexponential function, let $s \in C(x)$ be a shell of h and h_{ker} be the corresponding kernel (in the sense of Definition 3.70). Let $u, v \in C[x]$ be such that $\frac{h'}{h} = \frac{u}{v}$. Let $a, b, c \in C[x]$ be such that $s = \frac{a}{b} + \frac{c}{v}$, and assume that b is squarefree and coprime with v. Suppose there is a hypergeometric term g such that $h = g'$. Show that $b \mid a$.

23. Let h be a hypergeometric term, and let $u, v \in C[k]$ be such that $\frac{\sigma_k(h)}{h} = \frac{u}{v}$. Suppose that h is a kernel. Let $a, b, c \in C[k]$ be such that $(\frac{a}{b} + \frac{c}{v})h$ is Abramov-Petkovšek reduced.

a. Show that $\frac{h}{v}$ is also a kernel.

b. Show that $(\frac{av}{b} + c)\frac{h}{v}$ is Abramov-Petkovšek reduced.

24*. Show that the bound given in Theorem 5.62 on the order of the minimal telescoper of a proper hypergeometric term can undershoot arbitrarily much. More precisely, show that for every $r \in \mathbb{N}$ there is a proper hypergeometric for which Theorem 5.62 only predicts a telescoper of order "at least 0" while the minimal telescoper in fact has order at least r.

25*. Prove the following facts:

a. $\sum_k (-1)^k \binom{n}{k}\binom{k}{n} = (-1)^n$ and $\sum_k (-1)^k \binom{n}{k}\binom{n}{\ell} = 0$ for $\ell \neq n$.

b. For a polynomial $p \in C[x]$ of degree n, we have $\sum_k (-1)^k \binom{n}{k} p(n) = (-1)^n n! [x^n] p$.

c. $\sum_k (-1)^k \binom{n}{k}\binom{mk}{n} = (-m)^n$.

References

The classical text book [356] on hypergeometric summation contains a bound on the order of the telescoper which is extracted from the reasoning in the proof of Theorem 5.14. This bound is pessimistic. The approach reported here for obtaining better bounds was proposed by Apagodu and Zeilberger [35, 331]. They also discuss the q-case, the differential case, and the case of several variables, although in the case of several variables it remains unclear how to ensure that the telescoper is nonzero.

A generalization that applies to (almost) arbitrary D-finite input was developed by Chen, Kauers, and Koutschan [137] and also leads to a bound on the order of the telescoper in this case. There are some further bounds which do not depend on the Apagodu-Zeilberger approach. For example, for the case of algebraic functions, Chen, Kauers, and Singer [135] obtained a bound in terms of the dimension and the genus of the algebraic field extension in which the integrand lives. Also the reduction-based techniques discussed in the next section give rise to upper bounds on the order of telescopers.

Degree bounds depending on the order were worked out by Chen and Kauers in [128, 129], and the bound on the height was given by Kauers and Yen [275]. It improves the bound given by Yen in [463, 464], where she first proposed her two-line algorithm. Guo, Hou and Sun [227] proposed an interesting hybrid approach which for a given hypergeometric term performs some steps towards the computation of a telescoper with the aim of obtaining a better estimate for the largest integer root of the telescoper.

Abramov-Petkovšek reduction is due to Abramov and Petkovšek [17]. It was subsequently used for obtaining lower bounds by Abramov and Le [14]. A bound for the case when the summand is rational appears in [306]. Abramov-Petkovšek reduction is also the basis of Abramov's termination criterion of Zeilberger's algorithm [6, 7]. He shows that an irrational bivariate hypergeometric term f admits a telescoper if and only if Abramov-Petkovšek reduction rewrites it into $f = (\Delta_k \cdot g) + h$ for some term h which is proper hypergeometric. A termination analysis for the case of rational summation has appeared in [13]. Huang [242] obtains refined upper and lower bounds on the order of the telescoper by a variant of Abramov-Petkovšek reduction.

A differential version of Abramov-Petkovšek reduction for hyperexponential functions is given by Geddes, Le and Li in [207]. Our Exercise 22 is their Theorem 4. There is also a q-version [175]. The mixed case (terms depending on one discrete and one continuous variable) is discussed in [139]. Further information and additional references on bounds for creative telescoping can be found in Chyzak's habilitation thesis [156].

Example 5.65 is taken from the paper of Paule and Schorn [351]. Such examples are rare.

5.6 Reduction-Based Algorithms

Algorithms for creative telescoping can be divided into four generations. Algorithms of the first generation use elimination techniques in operator ideals as discussed in Sect. 5.2. An advantage of these algorithms is that they do not suffer from trouble with singularities. A disadvantage is that they are expensive. The second generation consists of Zeilberger's algorithm and its relatives as discussed in Sect. 5.4, which are based on a parameterized version of an algorithm for indefinite summation or integration. With the rise of these algorithms during the 1990s, the average computer overtook the average human as far as simplifying definite sums and integrals is concerned. The third generation of creative telescoping algorithms is obtained from the second generation by replacing the underlying indefinite summation/integration algorithm with linear algebra, as we have done in Sect. 5.5. Algorithms from this generation are easy to implement and easy to analyze but might fail to find the minimal telescoper.

In this final section, we shall discuss the most recent fourth generation of creative telescoping algorithms, the so-called class of reduction-based algorithms. The basic idea is again most easily explained for rational functions in the differential case. Let $p/q \in C(t)(x)$ and let $q^* \in C(t)[x]$ be the squarefree part of q. For every $i \in \mathbb{N}$, Hermite reduction can find $g_i \in C(t,x)$ and $u_i \in C(t)[x]$ such that

$$D_t^i \cdot \frac{p}{q} = (D_x \cdot g_i) + \frac{u_i}{q^*}$$

and $\deg_x(u_i) < \deg_x(q^*)$ for all i. Observe that the rational functions $\frac{u_i}{q^*}$ belong to the $C(t)$-vector space of dimension $\deg_x(q^*)$ which is generated by $1/q^*, \dots, x^{\deg_x(q^*)-1}/q^*$ in $C(t)(x)$, so that $1 + \deg_x(q^*)$ many of them must be linearly dependent over $C(t)$. In particular, for some $r \le \deg_x(q^*)$ there must be $c_0, \dots, c_r \in C(t)$, not all zero, such that

$$c_0 \frac{u_0}{q^*} + \cdots + c_r \frac{u_r}{q^*} = 0,$$

and for such a choice of $c_0, \ldots, c_r$, we have

$$(c_0 + \cdots + c_r D_t^r) \cdot \frac{p}{q} = D_x \cdot (c_0 g_0 + \cdots + c_r g_r),$$

so $c_0 + \cdots + c_r D_t^r$ is a telescoper for $\frac{p}{q}$.

Unless q can be written as a product of a univariate polynomial in t and a univariate polynomial in x, differentiation of $\frac{p}{q}$ with respect to either x or t increases the multiplicities of the factors of the denominator. This means that applying D_t^i to $\frac{p}{q}$ creates a lot of work during Hermite reduction, which has to eliminate all of the factors introduced by the differentiation. We can avoid some of this work. Instead of obtaining g_i, u_i by applying Hermite reduction to $D_t^i \cdot \frac{p}{q}$, we apply Hermite reduction to $D_t \cdot \frac{u_{i-1}}{q^*}$. If we write $\bar{g}_i, \bar{u}_i$ for the result, we have

$$D_t^i \cdot \frac{p}{q} = D_x((D_t \cdot g_{i-1}) + \bar{g}_i) + \frac{\bar{u}_i}{q^*},$$

which implies $\bar{u}_i = u_i$.

Example 5.66 For $\frac{p}{q} = \frac{1}{1+tx-x^3} \in C(t, x)$, we have

$$\begin{aligned} \frac{p}{q} &= (D_x \cdot g_0) + \frac{1}{1 + tx - x^3}, \\ D_t \cdot \frac{1}{1 + tx - x^3} &= (D_x \cdot g_1) + \frac{9x - 4t^2}{(4t^3 - 27)(1 + tx - x^3)}, \\ D_t^2 \cdot \frac{9x - 4t^2}{(4t^3 - 27)(1 + tx - x^3)} &= (D_x \cdot g_2) + \frac{2(135t + 16t^4 - 81t^2 x)}{(4t^3 - 27)^2(1 + tx - x^3)}, \end{aligned}$$

for certain $g_0, g_1, g_2 \in C(t, x)$. The ansatz

$$c_0 \frac{1}{1 + tx - x^3} + c_1 \frac{9x - 4t^2}{(4t^3 - 27)(1 + tx - x^3)} + c_2 \frac{2(135t + 16t^4 - 81t^2 x)}{(4t^3 - 27)^2(1 + tx - x^3)} = 0$$

leads to the linear system

$$\begin{pmatrix} (4t^3 - 27)^2 & -4t^2(4t^3 - 27) & 2t(16t^3 + 135) \\ 0 & 9(4t^3 - 27) & -162t^2 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = 0,$$

which has the nontrivial solution $(10t, 18t^2, 4t^3 - 27)$. Thus, $10t + 18t^2 D_t + (4t^3 - 27) D_t^2$ is a telescoper for $(1 + tx - x^3)^{-1}$. $\square$

This approach not only allows us to compute a telescoper for a given rational function $\frac{p}{q}$, but also offers an independent confirmation of the bound $r \leq \deg_x(q^*)$ on the order of the minimal telescoper that was derived in the previous section. An additional feature of this approach is that the linear systems that need to be solved for computing a telescoper are much smaller than in the approach used in the previous section, because we now do not make an ansatz for the certificate. Indeed, a key feature of the approach is that it allows us to compute a telescoper without also computing the corresponding certificate, which, as we have seen, may be much larger than the telescoper. Moreover, the approach finds the minimal telescoper of $\frac{p}{q}$. To see why, observe that Hermite reduction, viewed as a map $R\colon C(t, x) \to C(t, x)$, is $C(t)$-linear (Exercise 1), i.e., we have

$$\begin{aligned} R(c_0\frac{p}{q} + \cdots + c_r D_t^i \cdot \frac{p}{q}) &= c_0 R(\frac{p}{q}) + \cdots + c_r R(D_t^i \cdot \frac{p}{q}) \\ &= c_0\frac{u_0}{q^*} + \cdots + c_r\frac{u_r}{q^*}. \end{aligned}$$

As shown in Theorem 5.2, a rational function $f \in C(t, x)$ is integrable in $C(t, x)$ if *and only if* $R(f) = 0$. Therefore, choosing the $c_0, \ldots, c_r$ such that $c_0 u_0 + \cdots + c_r u_r = 0$ is not only sufficient but also necessary for $c_0 + \cdots + c_r D_t^r$ to be a telescoper of $\frac{p}{q}$.

It is worthwhile to formulate these observations in more general terms.

Definition 5.67 Let V be a K-vector space and U be a subspace of V. Let $R\colon V \to V$ be a K-linear map.

1. R is called a *reduction* for U if $v - R(v) \in U$ for all $v \in V$ and $\ker R \subseteq U$.
2. A reduction R is called *confined* if $\dim_K \mathrm{im} R < \infty$.
3. A reduction R is called *complete* if $\ker R = U$. □

Example 5.68 The case of rational functions discussed before can be matched to this definition as follows. Take $K = C(t)$ and fix a squarefree polynomial $\bar{q} \in K[x]$. Let $V \subseteq K(x)$ be the space of all rational functions whose denominators divide a power of $\bar{q}$. In other words, a rational function should belong to V if and only if every irreducible factor of its denominator is an irreducible factor of $\bar{q}$. Set $U = \{D_x \cdot f : f \in V\}$ and define $R\colon V \to V$ as follows. If Hermite reduction applied to some $f \in V$ returns g, h with $f = (D_x \cdot g) + h$, then we define $R(f) := h$.

By definition, we then have $f - R(f) \in U$ for all V. By Theorem 5.2, we also have $\ker R = U$. Finally, $\dim_K \mathrm{im} R < \infty$ because $\mathrm{im} R$ is generated by the elements $x^i/\bar{q}$ $(i = 0, \ldots, \deg_x(q) - 1)$. Therefore, R is a confined and complete reduction in the sense of Definition 5.67. □

Using the notion of reduction maps introduced in Definition 5.67, reduction-based telescoping can be formulated as follows.

Algorithm 5.69
Input: *An Ore algebra $K[\partial]$, a $K[\partial]$-module V, a submodule $U \subseteq V$, a reduction $R\colon V \to V$, and an element $f \in V$.*
Output: *A nonzero operator $P \in K[\partial]$ such that $P \cdot f \in U$.*

1 *Set* $h_0 = R(f)$.
2 *If* $h_0 = 0$, *return* 1.
3 *for* $r = 1, 2, \ldots,$ *do*
4   $h_r = R(\partial \cdot h_{r-1})$.
5   *Find* $c_0, \ldots, c_r \in K$ *such that* $c_0 h_0 + \cdots + c_r h_r = 0$.
6   *If there is a nonzero solution* $(c_0, \ldots, c_r) \in K^{r+1}$,
7   *return* $c_0 + c_1\partial + \cdots + c_r\partial^r$.

Theorem 5.70

1. *Algorithm 5.69 is correct.*
2. *If R is confined, Algorithm 5.69 terminates.*
3. *If R is complete, Algorithm 5.69 returns an operator P of smallest possible order.* □

Proof

1. First we show by induction on r that $(\partial^r \cdot f) - h_r \in U$ for all r. Since $R(f) - f \in U$ and $h_0 = R(f)$, we have $f - h_0 \in U$. Next, assuming that $(\partial^r \cdot f) - h_r \in U$, we have $(\partial^{r+1} \cdot f) - (\partial \cdot h_r) \in U$, because U is a $K[\partial]$-module. Using $R(\partial \cdot h_r) - (\partial \cdot h_r) \in U$ and $h_{r+1} = R(\partial \cdot h_r)$, it follows that $(\partial^{r+1} \cdot f) - h_{r+1} \in U$, as required.
   Now for $c_0, \ldots, c_r \in K$ with $c_0 h_0 + \cdots + c_r h_r = 0$ we have $c_0 f + \cdots + c_r(\partial^r \cdot f) \in U$, so the algorithm is correct.
2. The $h_0, \ldots, h_r$ computed by the algorithm all belong to $\operatorname{im} R$. By assumption, R is confined, which means that $\dim_K \operatorname{im} R < \infty$. Therefore, as soon as r exceeds $\dim_K \operatorname{im} R$, they must be linearly dependent over K, and the dependence will be detected in line 5.
3. We show the following: if $c_0, \ldots, c_r \in K$ are such that $(c_0 + \cdots + c_r\partial^r) \cdot f \in U$, then $c_0 h_0 + \cdots + c_r h_r = 0$. This implies that the algorithm cannot miss any operator P.
   $(c_0 + \cdots + c_r\partial^r) \cdot f \in U$ implies $R((c_0 + \cdots + c_r\partial^r) \cdot f) \in U$, which together with $\partial^i \cdot f - h_i \in U$ ($i \in \mathbb{N}$; cf. part 1) and $R(h_i) - h_i \in U$ ($i \in \mathbb{N}$) and the K-linearity of R implies $c_0 h_0 + \cdots + c_r h_r \in U$. The property $R(v) - v \in U = \ker R$ ($v \in V$) implies $R^2 = R$, which in turn implies $\ker R \cap \operatorname{im} R = \{0\}$. Therefore, since $h_i \in \operatorname{im} R$ for all i, we have $c_0 h_0 + \cdots + c_r h_r \in \ker R \cap \operatorname{im} R = \{0\}$, as claimed. ■

In particular, part 2 of the theorem implies the existence of an operator P as stated in the specification. In fact, there exists an operator of order $\dim_K \operatorname{im} R$. Part 3 does not imply existence, but if an operator P exists, then it implies the termination of the algorithm in this case.

The general formulation of Algorithm 5.69 is not limited to bivariate rational functions in the differential case but applies to every context for which we can provide a suitable reduction function. It can cover larger function classes, the summation case, as well as some multivariate settings. Here we discuss only two cases: multiple integration of rational functions and summation of hypergeometric terms.

We begin with rational functions. For a given $f \in C(x_1, \dots, x_n)$, the task is to find $g_1, \dots, g_n, h \in C(x_1, \dots, x_n)$ such that $f = (D_{x_1} \cdot g_1) + \cdots + (D_{x_n} \cdot g_n) + h$ and h is small in some sense. An immediate idea is to apply Hermite reduction repeatedly to the variables $x_1, \dots, x_n$ but this does not work very well (Exercise 3). It would be better if we could somehow handle all variables simultaneously, with Gröbner bases computations replacing the extended Euclidean algorithm. Following the univariate case, given $f = p/q^k$ for some squarefree polynomial q, we would need polynomials $b_1, \dots, b_n$ and c such that

$$\frac{p}{q^k} = \sum_{i=1}^{n} D_{x_i} \cdot \frac{b_i}{q^{k-1}} + \frac{c}{q^{k-1}}.$$

However, unlike in the univariate case, such polynomials do not always exist (Exercise 6). So we have to compromise. To make the equation solvable, we add an extra term u/q^k on the right hand side. An obvious solution is then $u = p$, $b_1 = \cdots = b_n = c = 0$, but there may be further solutions. We choose a solution in which u is minimal with respect to a prescribed term order. This can be done as follows.

Algorithm 5.71 *(Griffith-Dwork)*
Input: *A rational function $f \in C(x_1, \dots, x_n)$ and a Gröbner basis G of the ideal $\langle D_{x_1} \cdot q, \dots, D_{x_n} \cdot q\rangle \subseteq C[x_1, \dots, x_n]$, where q is the squarefree part of the denominator of f.*
Output: *$h \in C(x_1, \dots, x_n)$ such that there are $g_1, \dots, g_n \in C(x_1, \dots, x_n)$ with $f = \sum_{i=1}^n (D_{x_i} \cdot g_i) + h$.*

1 *Write $f = \frac{p}{q^k}$ for some $p \in C[x_1, \dots, x_n]$ and $k \in \mathbb{N}$ as small as possible. It is not required that p and q are coprime.*
2 *If $k = 0$, return 0.*
3 *If $k = 1$, return f.*
4 *Compute $u = \operatorname{red}(p, G)$ and $b_1, \dots, b_n \in C[x_1, \dots, x_n]$ such that $p = u + \sum_{i=1}^n b_i (D_{x_i} \cdot q)$.*
5 *Apply the algorithm recursively to $\frac{1}{(k-1)q^{k-1}} \sum_{i=1}^n (D_{x_i} \cdot b_i)$, and call the result h_0.*
6 *Return $\frac{u}{q^k} - h_0$.*

As it stands, the output specification of Algorithm 5.71 is not very useful yet, because it would also be satisfied by an algorithm that simply returns $g_1 = \cdots = g_n = 0$ and $h = f$. We will show in the next theorem that under additional assumptions on the input, the output is such that h is confined to a finite dimensional vector space.

Also observe that Algorithm 5.71 is not deterministic as formulated above, because the $b_1, \ldots, b_n$ chosen in line 4 are not uniquely determined and a different choice may lead to a different output (Exercise 7). We can make the algorithm deterministic by fixing a Gröbner basis G' of $\mathrm{Syz}(D_{x_1} \cdot q, \ldots, D_{x_n} \cdot q) \subseteq C[x_1, \ldots, x_n]^n$ and choosing in line 4, among all eligible vectors $(b_1, \ldots, b_n)$, the unique one which is in normal form with respect to G'. But even then, if we consider for a fixed q the function R that maps every rational function $f \in C(x_1, \ldots, x_n)$ of the form p/q^k to the rational function h returned by Algorithm 5.71 is not a reduction in the sense of Definition 5.67, because it fails to be linear. For example, $R(\frac{x}{x+y}) = \frac{x}{x+y}$ and $R(\frac{y}{x+y}) = \frac{y}{x+y}$ but $R(\frac{x}{x+y} + \frac{y}{x+y}) = R(1) = 0 \neq 1 = \frac{x}{x+y} + \frac{y}{x+y} = R(\frac{x}{x+y}) + R(\frac{y}{x+y})$. Despite this lack of linearity, we have the following variant of the confinement property.

Theorem 5.72

1. *Algorithm 5.71 is correct and terminates.*
2. *Let $q \in C[x_1, \ldots, x_n]$ be homogeneous of degree d. Suppose that $I = \langle D_{x_1} \cdot q, \ldots, D_{x_n} \cdot q\rangle \subseteq C[x_1, \ldots, x_n]$ is such that $\dim_C C[x_1, \ldots, x_n]/I < \infty$. Let $V \subseteq C(x_1, \ldots, x_n)$ be the C-vector space generated by all rational functions that can appear as output when Algorithm 5.71 is applied to p/q^k for some $k \in \mathbb{N}$ and some homogeneous polynomial $p \in C[x_1, \ldots, x_n]$. Then $\dim_C V < \infty$.* □

Proof

1. Termination follows from the fact that each recursive call in line 5 corresponds to a reduction of k, which ensures that the termination conditions in lines 2 and 3 are eventually satisfied. The correctness of the algorithm is clear if $k = 0$ or $k = 1$. For $k > 1$, we have to justify the calculations in lines 4 and 5. For the h_0 obtained in line 5, let $g_1, \ldots, g_n \in C(x_1, \ldots, x_n)$ be such that $\frac{1}{(k-1)q^{k-1}} \sum_{i=1}^n (D_{x_i} \cdot b_i) = \sum_{i=1}^n (D_{x_i} \cdot g_i) + h_0$. Then

$$\frac{p}{q^k} = \frac{u}{q^k} + \underbrace{\frac{1}{(k-1)q^{k-1}} \sum_{i=1}^n (D_{x_i} \cdot b_i) - \frac{1}{q^k} \sum_{i=1}^n b_i (D_{x_i} \cdot q)}_{=\sum_{i=1}^n D_{x_i} \cdot \frac{b_i}{(k-1)q^{k-1}}}$$

$$- \frac{1}{(k-1)q^{k-1}} \sum_{i=1}^n (D_{x_i} \cdot b_i)$$

$$= \sum_{i=1}^{n} (D_{x_i} \cdot (g_i + \frac{b_i}{(k-1)q^{k-1}})) + \frac{u}{q^k} - h_0.$$

This implies the correctness.

2. Since p and q are assumed to be homogeneous, the b_i computed in line 4 are homogeneous as well, and we have $\deg(b_i) = \deg(p) - \deg(D_{x_i} \cdot q) = \deg(p) + 1 - \deg(q)$ (unless $b_i = 0$ or $D_{x_i} \cdot q = 0$). Therefore, $\deg(D_{x_i} \cdot b_i) = \deg(p) - \deg(q)$, so the degree difference of the numerator and the denominator of the rational function formed in line 5 is equal to the degree difference of the numerator and the denominator of the input p/q^k. The final output thus has the form $\frac{u_k}{q^k} + \frac{u_{k-1}}{q^{k-1}} + \cdots + \frac{u_1}{q}$ for certain homogeneous polynomials $u_1, \ldots, u_k \in C[x_1, \ldots, x_n]$ where u_i has degree $\deg(p) - (k-i)\deg(q)$ (unless it is zero). Moreover, the polynomials $u_2, \ldots, u_k$ are in normal form with respect to G.

   As q is homogeneous, so are all its derivatives. Hence I is a homogeneous ideal. This implies that the normal form with respect to G of a polynomial of some degree s also has degree s. The terms which can appear in such normal forms form a C-vector space basis of $C[x_1, \ldots, x_n]/I$, and as this vector space has finite dimension by assumption, it follows that there exists some $m \in \mathbb{N}$, independent of p and k, such that $u_i = 0$ for all $i > m$.

   For any $i \in \mathbb{N}$, the number of terms of degree i in n variables is $\binom{n+i-1}{n}$, so the possible outputs $\frac{u_m}{q^m} + \cdots + \frac{u_1}{q}$ belong to a C-vector space of dimension at most $\sum_{i=1}^{m} \binom{n+i-1}{n} < \infty$. ■

Example 5.73

1. Consider $f = \frac{p}{q^3}$ with $p = x^4 + y^4$ and $q = x^2 + xy + y^2$. In the first iteration, we have

$$\frac{p}{q^3} = \frac{0}{q^3} - \frac{1}{6}(2x^3 - y^3)(D_x \cdot q^{-2}) + \frac{1}{6}(x^3 - 2y^3)(D_y \cdot q^{-2})$$
$$= -\frac{1}{6}(D_x \cdot \frac{2x^3 - y^3}{q^2}) + \frac{1}{6}\frac{6x^2}{q^2} + \frac{1}{6}(D_y \cdot \frac{x^3 - 2y^3}{q^2}) - \frac{1}{6}\frac{6y^2}{q^2}$$

   which reduces the problem to the integration of $\frac{x^2 - y^2}{q^2}$. In the second iteration, we write

$$\frac{x^2 + y^2}{q^2} = \frac{0}{q^2} - \frac{1}{3}(x - 3y)(D_x \cdot q^{-1}) - \frac{1}{3}(x + 3y)(D_y \cdot q^{-1})$$
$$= -\frac{1}{3}(D_x \cdot \frac{x - 3y}{q}) + \frac{1}{3}\frac{1}{q} - \frac{1}{3}(D_y \cdot \frac{x + 3y}{q}) + \frac{1}{q}$$

which reduces the problem to the integration of $\frac{4}{3q} = \frac{4}{3(x^2+xy+y^2)}$. This is when the algorithm stops because it has reached $k = 1$. The final output is $\frac{4}{3(x^2+xy+y^2)}$.

2. As an example for reduction-based telescoping, consider the rational function $f = \frac{p}{q^3}$ with $p = x^4 + ty^4$ and $q = x^2 + xy + ty^2$. We then have

$$R(\frac{p}{q^3}) = \frac{6t(t+1)}{(4t-1)^2}\frac{1}{q},$$

$$R(D_t \cdot \frac{p}{q^3}) = -\frac{6(2t^2+8t+1)}{(4t-1)^3}\frac{1}{q},$$

so a telescoper for f is $t(t+1)(4t-1)D_t + (2t^2+8t+1)$. □

Part 2 of Theorem 5.72 applies only to homogeneous polynomials p and q. The assumption that p be homogeneous can be relaxed quite easily. Every polynomial $p \in C[x_1, \ldots, x_n]$ can be written as a sum of homogeneous polynomials, and we can apply the algorithm to each of these separately and add up the results. In fact, in view of Exercise 5, it suffices to call the algorithm only on one of the homogeneous components of p.

If q is inhomogeneous, we can make it homogeneous by introducing an additional variable. For an arbitrary rational function $f \in C(x_1, \ldots, x_n)$ in n variables, we consider its *homogenization* $f_{\mathrm{hom}} := x_0^{-n-1} f(x_1/x_0, \ldots, x_n/x_0) \in C(x_0, \ldots, x_n)$. Note that f_{hom} is homogeneous of degree $-n-1$, because the quotients x_i/x_0 are homogeneous of degree 0, so $f(x_1/x_0, \ldots, x_n/x_0)$ is homogeneous of degree 0. (Recall that the degree of a rational function p/q is defined as $\deg(p) - \deg(q)$.) Of course, integrating f_{hom} with respect to $x_0, \ldots, x_n$ is not the same as integrating f with respect to $x_1, \ldots, x_n$. What matters for us is that any telescoper of f_{hom} is a telescoper of f.

Proposition 5.74 *Let $f \in C(t)(x_1, \ldots, x_n)$. Then every telescoper $P \in C(t)[D_t]$ that reduction-based telescoping with Algorithm 5.71 finds for*

$$f_{\mathrm{hom}} = x_0^{-n-1} f(x_1/x_0, \ldots, x_n/x_0)$$

is also a telescoper of f. □

Proof Let $g_0, \ldots, g_n \in C(x_0, \ldots, x_n)$ be such that $P \cdot f_{\mathrm{hom}} = \sum_{i=0}^n (D_{x_i} \cdot g_i)$. By the assumption that P was found using Algorithm 5.71, we can assume that $g_0, \ldots, g_n$ are homogeneous. Since the degree of f_{hom} is $-n-1$, we may further assume that the degrees of $g_0, \ldots, g_n$ are $-n$. Setting x_0 to 1 gives $P \cdot f = (D_{x_0} g_0)|_{x_0=1} + \sum_{i=1}^n (D_{x_i} \cdot g_i|_{x_0=1})$, so it remains to show that $(D_{x_0} \cdot g_0)|_{x_0=1}$ is integrable with respect to $x_1, \ldots, x_n$. By Exercise 4, we have

$$\sum_{i=1}^{n} D_{x_i} \cdot (x_i g_0|_{x_0=1}) = \sum_{i=1}^{n} g_0|_{x_0=1} + \sum_{i=1}^{n} x_i (D_{x_i} g_0|_{x_0=1})$$
$$= (n + (-n)) g_0|_{x_0=1} - (D_{x_0} \cdot g_0)|_{x_0=1},$$

so $(D_{x_0} \cdot g_0)|_{x_0=1} = -\sum_{i=1}^{n} D_{x_i} \cdot (x_i g_0|_{x_0=1})$, as required. ∎

There remains the question of what to do if $\dim_C C[x_1, \dots, x_n]/I$ is infinite. This situation can be settled by introducing a new variable x_0 to the ground field. The idea is to replace the denominator q with $\bar{q} = q + x_0(x_1^d + \cdots + x_n^d)$. It can then be shown that

$$\dim_{C(x_0)} C(x_0)[x_1, \dots, x_n]/\langle D_{x_1} \cdot \bar{q}, \dots, D_{x_n} \cdot \bar{q} \rangle < \infty.$$

Moreover, if we compute a telescoper for $p/\bar{q}$, then setting x_0 to zero in the telescoper gives a telescoper for p/q. For more details and alternative approaches to deal with the situation when $\dim_C C[x_1, \dots, x_n]/I$ is infinite, we refer to the literature.

Let us now turn to the case of hypergeometric summation. Our goal is to design a reduction in the sense of Definition 5.67 based on the Abramov-Petkovšek reduction introduced in the previous section. As it stands, Algorithm 5.59 does not define a reduction. One problem is that a given hypergeometric term f can be written in several ways in the form $f = (\Delta_k \cdot g) + h$ for some Abramov-Petkovšek reduced term h. For example, if $h = (\frac{a}{b} + \frac{c}{v}) f_{\mathrm{ker}}$ is Abramov-Petkovšek reduced then so is

$$h + (\Delta_k \cdot f) = \Big(\frac{a}{b} + \frac{c}{v} + \frac{u}{v} - 1\Big) f_{\mathrm{ker}} = \Big(\frac{a-b}{b} + \frac{c+u}{v}\Big) f_{\mathrm{ker}}.$$

We shall add a post-processing step to Algorithm 5.59 with the aim of minimizing the polynomials a and c. First, because of $\frac{a}{b} + \frac{c}{v} = \frac{\mathrm{rem}(a,b)}{b} + \frac{\mathrm{quo}(a,b)v+c}{v}$, we can replace a and c by $\mathrm{rem}(a, b)$ and $\mathrm{quo}(a, b)v + c$, respectively, to ensure that $\deg_k(a) < \deg_k(b)$. Note that Proposition 5.58 implies that an Abramov-Petkovšek reduced term with $\deg_k(a) < \deg_k(b)$ can only be summable if $a = 0$. Next, we eliminate as many monomials as possible from c, but of course without moving them back to a. Instead, we want to move them into $\Delta_k \cdot g$. If there is a polynomial p such that $u\sigma_k(p) - vp = c$, we can move all of c into $\Delta_k \cdot g$, because then we have

$$\Delta_k \cdot p f_{\mathrm{ker}} = \Big(\frac{\sigma_k(p)u}{v} - p\Big) f_{\mathrm{ker}} = \frac{c}{v} f_{\mathrm{ker}}.$$

In general, such a polynomial p does not exist. We can then think of c as a sum of two polynomials, one of which can be eliminated and the other can not. In this decomposition, we want the part that can be eliminated to be as large as possible. This can be arranged as follows.

For the linear map $\varphi\colon C[k] \to C[k]$ defined by $\varphi(p) = u\sigma_k(p) - vp$, choose a subspace W of $C[k]$ such that $C[k] = \operatorname{im}\varphi \oplus W$. (See Exercise 11 for how to do this.) Then c can be written uniquely as $c = c_0 + c_1$ for some $c_0 \in \operatorname{im}\varphi$ and some $c_1 \in W$. By definition of φ, we can eliminate c_0 from c.

Example 5.75 Let $f_{\text{ker}} = \binom{2k}{k}$, so that $u = 4k + 2$ and $v = k + 1$. For every $e \in \mathbb{N}$, we have $\varphi(k^e) = (4k + 2)(k + 1)^e - (k + 1)k^e = 3k^{e+1} + \mathrm{O}(k^e)$. Therefore, the image of φ contains polynomials of any positive degree but not of degree zero. We can thus choose W as the vector space generated by 1.

1. Consider $h = (\frac{0}{1} + \frac{(2k+1)(3k+4)}{v}) f_{\text{ker}}$. The term h is Abramov-Petkovšek reduced. We want to find $c_0 \in \operatorname{im}\varphi$ and $c_1 \in W$ such that $(2k + 1)(3k + 4) = c_0 + c_1$. We make an ansatz $c_0 = \varphi(c_{0,0} + c_{0,1}k) = (c_{0,0} + 2c_{0,1}) + (3c_{0,0} + 5c_{0,1})k + 3c_{0,1}k^2$ with undetermined coefficients $c_{0,0}, c_{0,1} \in C$ and equate the coefficients of $(2k + 1)(3k + 4) - (c_0 + c_1)$ to zero. The resulting system has the unique solution $c_0 = 2k + \frac{1}{3}$, $c_1 = -\frac{1}{3}$.
   It follows that $h = (\Delta_k \cdot (2k + \frac{1}{3}) f_{\text{ker}}) + (\frac{0}{1} - \frac{1/3}{k+1}) f_{\text{ker}}$. Thus, we have found the simplification
   $$\sum_{k=0}^{n} \frac{(2k+1)(3k+4)}{k+1}\binom{2k}{k} = \frac{1}{3}(6n+7)\binom{2(n+1)}{n+1} - \frac{1}{3} - \frac{1}{3}\sum_{k=0}^{n}\frac{1}{k+1}\binom{2k}{k}.$$
   It can be checked with Gosper's algorithm and it also follows from Theorem 5.77 below that h is not summable.
2. Now consider the term $h = (\frac{0}{1} + \frac{(2k+1)(3k+5)}{v}) f_{\text{ker}}$, which also is Abramov-Petkovšek reduced. We proceed as before and find $(2k + 1)(3k + 5) = \varphi(2k + 1) + 0$. This means that $h = \Delta_k \cdot (2k + 1)\binom{2k}{k}$, so in this case, we find that h is summable. □

The procedure just described is called polynomial reduction and can be summarized as follows.

Algorithm 5.76 *(Polynomial reduction)*
Input: *A hypergeometric term* $f = s f_{\text{ker}}$ *with* $s \in C(k)$ *and* f_{ker} *a kernel with* $u, v \in C[k]$ *such that* $\sigma_k(f_{\text{ker}})/f_{\text{ker}} = u/v$. *A subspace* $W \subseteq C[k]$ *such that for the linear map* $\varphi\colon C[k] \to C[k]$ *defined by* $\varphi(p) = u\sigma_k(p) - vp$ *we have* $C[k] = \operatorname{im}\varphi \oplus W$.
Output: $a, b, c \in C[k]$ *such that* $\deg_k(a) < \deg_k(b)$, $c \in W$, $h = (\frac{a}{b} + \frac{c}{v}) f_{\text{ker}}$ *is Abramov-Petkovšek reduced, and* $f = (\Delta_k \cdot g) + h$ *for some hypergeometric term* g.

1 *Use Algorithm 5.59 to compute* $a, b, c \in C[k]$ *such that* $h = (\frac{a}{b} + \frac{c}{v}) f_{\text{ker}}$ *is Abramov-Petkovšek reduced and* $f = (\Delta_k \cdot g) + h$ *for some hypergeometric term* g.
2 *Set* $c = \operatorname{quo}(a, b)v + c$ *and* $a = \operatorname{rem}(a, b)$.
3 *Write* $c = c_0 + c_1$ *with* $c_0 \in \operatorname{im}\varphi$ *and* $c_1 \in W$.
4 *Return* $(\frac{a}{b} + \frac{c_1}{v}) f_{\text{ker}}$.

Theorem 5.77 *Algorithm 5.76 is correct. Moreover, applied to a hypergeometric term f, the algorithm returns zero if and only if f is summable.* □

Proof Because of $\frac{a}{b} + \frac{c}{v} = \frac{\operatorname{rem}(a,b)}{b} + \frac{\operatorname{quo}(a,b)v+c}{v}$, the change made in line 2 does not change the h obtained in line 1 but only writes it differently. The new form still meets the requirements of Definition 5.57, as these requirements only depend on b, u, v but not on a, c. In line 3, c_0 is chosen so that there is a $p \in C[k]$ with $u\sigma_k(p) - vp = c_0$. For any such p we have $\Delta_k \cdot pf_{\text{ker}} = \frac{c_0}{v} f_{\text{ker}}$, which allows us to translate $f = \Delta_k \cdot g + (\frac{a}{b} + \frac{c_0+c_1}{v}) f_{\text{ker}}$ into $f = \Delta_k(g + pf_{\text{ker}}) + (\frac{a}{b} + \frac{c_1}{v}) f_{\text{ker}}$. Again, changing c to c_1 does not affect the requirements of Definition 5.57, which only depend on b, u, v. Therefore, the term returned in line 4 has all of the promised properties, so the algorithm is correct.

It is clear that f is summable if the algorithm returns zero, because then we have $f = \Delta_k \cdot g + 0$ for some g. For the converse, let $h = (\frac{a}{b} + \frac{c_1}{v}) f_{\text{ker}}$ be a summable output of Algorithm 5.76. We have to show that h is zero. If $a \neq 0$, then it follows from Proposition 5.58 that h is not summable because the condition $\deg_k(a) < \deg_k(b)$ together with $a \neq 0$ implies $b \nmid a$. So we have $a = 0$. If $p, q \in C[k]$ are such that $h = \Delta_k \cdot \frac{p}{q} f_{\text{ker}}$, then $u\sigma_k(\frac{p}{q}) - v\frac{p}{q} = c_1$. Since f_{ker} is a kernel, we have $\gcd(\sigma^i(u), v) = 1$ for all $i \in \mathbb{Z}$. Therefore, Theorem 2.62 implies that $\frac{p}{q} \in C[x]$. But then $c_1 = u\sigma_k(\frac{p}{q}) - v\frac{p}{q} = \varphi(\frac{p}{q}) \in \operatorname{im}\varphi$ and $c_1 \in W$ and $\operatorname{im}\varphi \cap W = \{0\}$ force $c_1 = 0$. Thus $h = 0$, as claimed. ■

Although the output specification of Algorithm 5.76 imposes stronger restrictions on h than that of the original Abramov-Petkovšek reduction, it still does not determine h uniquely. For example, the two terms $h = (\frac{1}{k} + \frac{0}{1})2^k$ and $\tilde{h} = (\frac{1}{2(k-1)} + \frac{0}{1})2^k$ both meet all of the requirements and their difference $h - \tilde{h} = \Delta_k \frac{1}{2(k-1)} 2^k$ is summable, so if h is a correct output for a certain hypergeometric term f, then $\tilde{h}$ would be a correct output as well. Because of this non-uniqueness, we cannot expect that the function which maps a given hypergeometric term f to the output of Algorithm 5.76 is C-linear. For example, $h = (\frac{1}{k} + \frac{0}{1})2^k$ may be the output for some term f and $\tilde{h} = (\frac{1}{2(k-1)} + \frac{0}{1})2^k$ may be the output for some other term $\tilde{f}$, but there is no way that the output for $f - \tilde{f}$ is $h - \tilde{h}$.

The problem can be fixed by imposing even further constraints. Recall that two polynomials $p, q \in C[k]$ are called shift-equivalent if $\sigma_k^i(p) = q$ for some $i \in \mathbb{Z}$ (Definition 2.60). Definition 5.57 requires that the monic irreducible factors of b should be pairwise not shift equivalent, i.e., they should belong to different equivalence classes. A remaining degree of freedom is that Definition 5.57 does not specify which element of an equivalence should appear in b. In fact, we can choose the representative freely. To see this, consider a hypergeometric term $h = (\frac{a}{b} + \frac{c}{v}) f_{\text{ker}}$ that meets the conditions in the output specification of Algorithm 5.76. Let p be a monic irreducible factor of b, and write $b = \tilde{b}p^e$ for some $\tilde{b} \in C[k]$ which does not contain p. Then $\frac{a}{b} = \frac{a_1}{\tilde{b}} + \frac{a_2}{p^e}$ for certain $a_1, a_2 \in C[k]$, and $\frac{\sigma_k(a_1)u}{\sigma_k(p)^e v} = \frac{a_3}{\sigma_k(p)^e} + \frac{a_4}{v}$ for certain $a_3, a_4 \in C[k]$. Therefore,

$$\begin{aligned} h + (\Delta_k \cdot \frac{a_2}{p^e} f_{\mathrm{ker}}) &= \Big(\frac{a}{\tilde{b} p^e} + \frac{c}{v} + \frac{\sigma_k(a_2)u}{\sigma_k(p)^e v} - \frac{a_2}{p^e}\Big) f_{\mathrm{ker}} \\ &= \Big(\frac{a_1}{\tilde{b}} + \frac{a_2}{p^e} - \frac{a_2}{p^e} + \frac{a_3}{\sigma_k(p)^e} + \frac{c}{v} + \frac{a_4}{v}\Big) f_{\mathrm{ker}} \\ &= \Big(\frac{a_1 \sigma_k(p)^e + \tilde{b} a_3}{\tilde{b} \sigma_k(p)^e} + \frac{c + a_4}{v}\Big) f_{\mathrm{ker}}. \end{aligned}$$

By repeating the calculation, we can move the factor p^e forward as far as we like, and by a similar calculation, we can also shift it backwards. The new numerators might no longer meet the output conditions of Algorithm 5.76, but we can restore them by executing lines 2–4 of the algorithm, which don't spoil the adjustments we made to b.

Summarizing, we see that for every shift-equivalence class we can decide freely which of its elements (if any) shows up in b. We can use this freedom to constrain h further by selecting one element from each class and requesting that only selected elements shall occur in b. The following theorem says that h is then uniquely determined.

Theorem 5.78 *Let $P \subseteq C[k]$ be a set of representatives of the shift-equivalence classes of all monic irreducible polynomials. In other words, P should be a set of monic irreducible polynomials such that no two elements of P are shift-equivalent and for every monic irreducible polynomial $p \in C[k]$, there is an $i \in \mathbb{Z}$ such that $\sigma_k^i(p) \in P$.*

Let f_{ker} be a kernel and $u, v \in C[k]$ be such that $\sigma_k(f_{\mathrm{ker}})/f_{\mathrm{ker}} = u/v$. Let $W \subseteq C[k]$ be such that $C[k] = \operatorname{im}\varphi \oplus W$ for the linear map $\varphi\colon C[k] \to C[k]$, $\varphi(p) = u\sigma_k(p) - vp$.

Let f be a hypergeometric term with kernel f_{ker}. Then there exists exactly one hypergeometric term h with the following properties:

1. *$h = (\frac{a}{b} + \frac{c}{v}) f_{\mathrm{ker}}$ for some $a, b, c \in C[k]$ and $f = (\Delta_k \cdot g) + h$ for some hypergeometric term g.*
2. *h is Abramov-Petkovšek reduced, i.e., a, b, c satisfy the conditions of Definition 5.57.*
3. *Every irreducible factor of b belongs to P.*
4. *$\deg_k(a) < \deg_k(b)$ and $c \in W$.*

If $V = C(k) f_{\mathrm{ker}}$ is the C-vector space of all hypergeometric terms f with kernel f_{ker}, then the map $R\colon V \to V$ which maps f to the uniquely determined h with the above properties is a complete reduction for $U := \{\, \Delta_k \cdot g : g \in V \,\}$. □

Proof The existence of a hypergeometric term h with the desired properties follows from the fact that we can compute one, as follows. Algorithm 5.59 applied to f produces a term $h = (\frac{a}{b} + \frac{c}{v}) f_{\mathrm{ker}}$ which meets the first two requirements. Next, using calculations as described above, we can turn this term into one of the same form but with a b whose irreducible factors all belong to P. The resulting term meets the first three requirements. Finally, by executing lines 2–4 of Algorithm 5.76, we can get a term that additionally meets the fourth requirement.

For the uniqueness, consider two terms $h = (\frac{a}{b} + \frac{c}{v}) f_{\text{ker}}$, $\tilde{h} = (\frac{\tilde{a}}{\tilde{b}} + \frac{\tilde{c}}{v}) f_{\text{ker}}$ that meet the conditions of the theorem. Then for two hypergeometric terms $g, \tilde{g}$ we have $f = (\Delta_k \cdot g) + h$ and $f = (\Delta_k \cdot \tilde{g}) + \tilde{h}$, so $\Delta_k \cdot (\tilde{g} - g) = h - \tilde{h}$, so $h - \tilde{h}$ is summable. However, as the irreducible factors of b and $\tilde{b}$ are constrained to the set P, so are the irreducible factors of $\operatorname{lcm}(b, \tilde{b})$. Therefore, the term

$$h - \tilde{h} = \Big(\frac{(a\tilde{b} - \tilde{a}b)/\gcd(b, \tilde{b})}{\operatorname{lcm}(b, \tilde{b})} + \frac{c - \tilde{c}}{v}\Big) f_{\text{ker}}$$

meets the conditions in the output specification of Algorithm 5.76. By Theorem 5.77, the summability of $h - \tilde{h}$ implies $h - \tilde{h} = 0$. This completes the uniqueness.

It remains to show that R is a complete reduction. To see that R is linear, let $\alpha_1, \alpha_2 \in C$, $f_1, f_2 \in V$. We claim that $R(\alpha_1 f_1 + \alpha_2 f_2) = \alpha_1 R(f_1) + \alpha_2 R(f_2)$. The argument is the same as before: if b_1, b_2 are the polynomials playing the role of b in $R(f_1)$, $R(f_2)$, respectively, their irreducible factors are constrained to P, so the irreducible factors of $\operatorname{lcm}(b_1, b_2)$ also belong to P. Therefore, $\alpha_1 R(f_1) + \alpha_2 R(f_2)$ meets the four conditions stated in the theorem, and it follows from here that it is equal to $R(\alpha_1 f_1 + \alpha_2 f_2)$. It is clear that $f - R(f) \in U$ for all $f \in V$, and, by Theorem 5.77, that $\ker R = U$. Therefore, R is a complete reduction. ∎

Now that we have a complete reduction for hypergeometric terms, we can use Algorithm 5.69 to compute telescopers for bivariate hypergeometric terms. Here, $C(n)$ takes the role of the constant field C. In practice and in implementations, it is not necessary to fix the set P beforehand. Instead, it may be more convenient and more efficient to choose it on the fly. We compute $h_0 = R(f)$ without any preference for which shift-equivalence class representatives should appear in b. In the computation of $h_i = R(\partial \cdot h_{i-1})$ for $i > 0$, we forbid all irreducible factors which are shift-equivalent to, but distinct from, irreducible factors appearing in the b's of $h_0, \ldots, h_{i-1}$.

Example 5.79

1. For $f = f_{\text{ker}} = \binom{n}{k}$ we have $u = -k + n$ and $v = k + 1$, and we can take as W the $C(n)$-vector space generated by 1. Then

$$R(\binom{n}{k}) = \Big(\frac{0}{1} + \frac{(n+1)/2}{k+1}\Big)\binom{n}{k},$$

$$R(\binom{n+1}{k}) = \Big(\frac{0}{1} + \frac{n+1}{k+1}\Big)\binom{n}{k},$$

and we see the linear dependence $R(\binom{n+1}{k}) - 2R(\binom{n}{k}) = 0$ which translates into the well-known telescoper $S_n - 2$ for $\binom{n}{k}$. The set P does not play any role in this example.

2. With $f_{\mathrm{ker}}, u, v, W$ as above, consider now $f = \frac{1}{k+n} f_{\mathrm{ker}}$. We can take

$$R(f) = \Bigl(\frac{1}{k+n} + \frac{0}{k+1}\Bigr)\binom{n}{k}$$

and thereby decide that P should contain $k+n$. Once this decision is made,

$$R(S_n \cdot f) = \Bigl(\frac{-n/(2+4n)}{k+n} + \frac{(3n+2)/(4n+2)}{k+1}\Bigr)\binom{n}{k}$$

is uniquely determined, because b does not contain any factors outside of the shift-equivalence class of $n+k$. If there were any, we would leave them as they are and declare them as additional elements of P.
In the next step, we get

$$R(S_n^2 \cdot f) = \Bigl(\frac{a}{k+n} + \frac{c}{k+1}\Bigr)\binom{n}{k}$$

with

$$a = \frac{n(n+1)}{4(2n+1)(2n+3)} \quad \text{and} \quad c = \frac{(n+1)(21n^2+44n+16)}{4(n+2)(2n+1)(2n+3)}$$

and we now find a linear relation that translates into the telescoper

$$2n(n+1)(3n+5)+(n+1)(21n^2+44n+16)S_n-2(n+2)(2n+3)(3n+2)S_n^2$$

for f. □

One of the main features of reduction-based telescoping is that it allows us to construct a telescoper without also constructing a corresponding certificate. This is desirable because certificates may be much larger than telescopers, so by avoiding their computation, we can expect to save a lot of time. A downside of saving the time for computing the certificate is that the approach is limited to situations where a certificate is not needed. This is the case for the closure properties discussed in Theorems 5.31 and 5.33, which are based on extracting residues of formal Laurent series in several variables. For hypergeometric summation, not knowing the certificate is more problematic, even in the case of natural boundaries, because it might have singularities in the summation range, and in this case, we are in general not entitled to conclude that the telescoper for a summand annihilates the sum.

An alternative approach to hypergeometric summation which allows us to take advantage of reduction-based techniques consists of translating the summation problem at hand into a residue extraction problem. Such a translation cannot be done for every hypergeometric sum, but it can be done for many sums that appear in applications, including nested sums. The sequences to which the approach applies are called binomial sums. They are defined as follows.

Definition 5.80 The class of *binomial sums* is inductively defined by the following rules:

1. $(\delta_{n,0})_{n\in\mathbb{Z}}$ is a binomial sum.
2. For every $q \in C \setminus \{0\}$, the geometric sequence $(q^n)_{n\in\mathbb{Z}}$ is a binomial sum.
3. The binomial coefficient sequence $(\binom{n}{k})_{n,k\in\mathbb{Z}}$ is a binomial sum.
4. The product and any C-linear combination of two binomial sums are binomial sums.
5. If $(a_{k_1,\dots,k_e})_{k_1,\dots,k_e\in\mathbb{Z}}$ is a binomial sum and $\lambda\colon \mathbb{Z}^d \to \mathbb{Z}^e$ is an affine map, then the sequence $(a_{\lambda(n_1,\dots,n_d)})_{n_1,\dots,n_d\in\mathbb{Z}}$ is a binomial sum.
6. If $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{Z}}$ is a binomial sum, then so is $(b_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{Z}}$ defined by

$$b_{n_1,\dots,n_d} = \sum_{k=0}^{n_d} a_{n_1,\dots,n_{d-1},k}$$

with the usual convention that the sum is zero for $n_d < 0$.

For $D \subseteq \mathbb{Z}^d$, a function $a\colon D \to C$ is called a binomial sum if there is a binomial sum $b\colon \mathbb{Z}^d \to C$ with $a(n_1,\dots,n_d) = b(n_1,\dots,n_d)$ for all $(n_1,\dots,n_d) \in D$. ◻

As an alternative to rule 6, we can employ the so-called *directed sum,* which is defined via

$$\sum_{k=a}^{b}{}' u_k = \begin{cases} \sum_{k=a}^{b} u_k & \text{if } a \le b,\\ 0 & \text{if } a = b+1,\\ -\sum_{k=b+1}^{a-1} u_k & \text{if } a > b+1, \end{cases}$$

for any sequence $(u_k)_{k\in\mathbb{Z}}$ and any $a, b \in \mathbb{Z}$. The directed sum is sometimes computationally easier. Because of

$$\sum_{k=a}^{b}{}' u_k = \sum_{k=a}^{b} u_k - \sum_{k=-a}^{-(b+1)} u_{-k} + u_a \sum_{k=-a}^{-(b+1)} \delta_{k+a},$$

the rules 1, 4, 5, and 6 show that the class of binomial sums is also closed under directed sums. Conversely, the standard sum can be expressed in terms of the directed sum via $\sum_{k=0}^{n} a_n = h_n \sum_{k=0}^{\prime\, n} a_n$ with $h_n := \sum_{k=0}^{\prime\, n} \delta_k$. Note that $h_n = 1$ for $n \ge 0$ and $h_n = 0$ for $n < 0$. As either can be expressed in terms of the other, we are free to replace the standard sum by the directed sum in rule 6 of the definition.

Here are some further sequences that belong to the class of binomial sums.

Example 5.81

1. Polynomial sequences are binomial sums, because $(1)_{n\in\mathbb{Z}}$ is a binomial sum by rule 2, thus $(n)_{n\in\mathbb{Z}}$ is a binomial sum by $n = \sum_{k=0}^{\prime\, n} 1$ (rule 6), and therefore $(p(n))_{n\in\mathbb{Z}}$ is a binomial sum for every polynomial p by rule 4. More generally, $(p(n_1,\dots,n_d))_{n_1,\dots,n_d\in\mathbb{Z}}$ is a binomial sum for every polynomial p in d variables.
2. The sequence $(C_n)_{n=0}^{\infty}$ of Catalan numbers is a binomial sum, because $C_n = \binom{2n}{n} - \binom{2n}{n+1}$ for all $n \in \mathbb{N}$. Note that the formula $C_n = \frac{1}{n+1}\binom{2n}{n}$ does not help directly, because the sequence $(\frac{1}{n+1})_{n=0}^{\infty}$ is not a binomial sum (Exercise 18).
3. The sequence $\sum_{i=0}^{n}\sum_{j=0}^{n}\binom{i+j}{i}^2\binom{4n-2i-2j}{2n-2i}$ is a binomial sum. This does not only follow from the fact that the sum is equal to $(2n+1)\binom{2n}{n}^2$, but it can also be seen from the sum expression: by rules 3 and 5, the binomials $\binom{i+j}{i}$ and $\binom{4n-2i-2j}{2n-2i}$, viewed as sequences in $i, j, n \in \mathbb{Z}$, are binomial sums. With rule 4 it then follows that the whole summand is a binomial sum. By rule 6, we get that $\sum_{i=0}^{a}\sum_{j=0}^{b}\binom{i+j}{i}^2\binom{4n-2i-2j}{2n-2i}$ is a binomial sum as a sequence in $a, b, n \in \mathbb{Z}$. Finally, rule 5 lets us set $a = b = n$.
4. Let $v_1,\dots,v_\ell \in \mathbb{Q}^d$, and for every $i = 1,\dots,\ell$, let $H_i = \{x \in \mathbb{R}^d : x\cdot v_i \geq 0\} \subseteq \mathbb{R}^d$ be the half space whose supporting hyperplane has v_i as normal vector. Let $K = \bigcap_{i=1}^{\ell} H_i$ be the intersection of these half spaces. Define $a_{n_1,\dots,n_d} = 1$ if $(n_1,\dots,n_d) \in K$ and $a_{n_1,\dots,n_d} = 0$ otherwise. Then the sequence $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{Z}}$ is a binomial sum. Because of rule 4, it suffices to consider the case $\ell = 1$, i.e., $K = H_1$. Because of rule 5 and the fact that the v_i have rational coordinates, it suffices to consider the case $v_1 = (1,0,\dots,0)$, i.e., $a_{n_1,\dots,n_d} = 1$ if $n_1 \geq 0$ and $a_{n_1,\dots,n_d} = 0$ otherwise. Because of $a_{n_1,\dots,n_d} = \sum_{k=0}^{n_1}\delta_k$, the sequence being a binomial sum follows from rules 1 and 6.
5. The diagonal of the formal power series $\frac{1}{1-(x^2+xy-y^2)}$ is a binomial sum, because we have

$$
\begin{aligned}
&[x^n y^n]\frac{1}{1-(x^2+xy-y^2)}\\
&= [x^n y^n]\sum_{k=0}^{\infty}(x^2+xy-y^2)^k\\
&= [x^n y^n]\sum_{k=0}^{\infty}\sum_{i}\binom{k}{i}x^{2i}(xy-y^2)^{k-i}\\
&= [x^n y^n]\sum_{k=0}^{\infty}\sum_{i}\sum_{j}\binom{k}{i}\binom{i}{j}(-1)^{k-i-j}\underbrace{x^{2i}(xy)^j y^{2(k-i-j)}}_{=x^{2i+j}y^{2k-2i-j}}\\
&= \sum_{i}(-1)^{n-i-(n-2i)}\binom{n}{i}\binom{i}{n-2i},
\end{aligned}
$$

and the latter expression can be formed by the rules of Definition 5.80. It can be shown more generally that the diagonal of any rational formal power series is a binomial sum. □

As we have seen in Sect. 5.3, a sequence can be expressed as a diagonal of a rational function if and only if it can be expressed as a residue of a rational function. Therefore, every sequence that can be expressed as a residue of a rational function is a binomial sum. The following theorem provides a converse.

Theorem 5.82 *For every binomial sum $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{N}}$ there is a rational function $r \in C(t_1,\dots,t_d,x_1,\dots,x_e)$ such that*

$$\sum_{n_1,\dots,n_d\in\mathbb{N}} a_{n_1,\dots,n_d} t_1^{n_1}\cdots t_d^{n_d} = \operatorname{Res}_{x_1,\dots,x_e} r(t_1,\dots,t_d,x_1,\dots,x_e),$$

where the rational function r is viewed as an element of $C_\le((t_1,\dots,t_d,x_1,\dots,x_e))$ for a suitable term order $\le$.

In particular, every binomial sum $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{N}}$ is holonomic. □

Proof The second claim follows from the first by Theorem 5.31. We show the first claim by checking that it is preserved by the rules stated in Definition 5.80.

1. $\sum_{n\in\mathbb{N}} \delta_n t^n = 1 = \operatorname{Res}_x \frac{1}{x}$.
2. $\sum_{n\in\mathbb{N}} q^n t^n = \frac{1}{1-qt} = \operatorname{Res}_x \frac{1}{(1-qt)x}$.
3. $\sum_{n,k\in\mathbb{N}} \binom{n}{k} t_1^k t_2^n = \sum_{n=0}^\infty (1+t_1)^n t_2^n = \frac{1}{1-(1+t_1)t_2} = \operatorname{Res}_x \frac{1}{(1-(1+t_1)t_2)x}$.
4. Closure under C-linear combinations follows from the linearity of the residue operator. Closure under multiplication follows from

$$\begin{aligned} &a(t_1,\dots,t_d) \odot_{t_1,\dots,t_d} b(t_1,\dots,t_d) \\ &= \operatorname{Res}_{\tau_1,\dots,\tau_d} \frac{1}{\tau_1\cdots\tau_d} a(\tau_1,\dots,\tau_d) b\Big(\frac{t_1}{\tau_1},\dots,\frac{t_d}{\tau_d}\Big). \end{aligned}$$

5. Let $\lambda\colon \mathbb{Z}^d \to \mathbb{Z}^e$, $\lambda(n) := \Lambda n + \mu$ be an affine map defined through a matrix $\Lambda = ((\lambda_{i,j}))_{i,j=1}^{e,d} \in \mathbb{Z}^{e\times d}$ and a vector $\mu = (\mu_1,\dots,\mu_e) \in \mathbb{Z}^e$. If $(a_{k_1,\dots,k_e})_{k_1,\dots,k_e\in\mathbb{N}}$ is such that

$$\sum_{k_1,\dots,k_e\in\mathbb{N}} a_{k_1,\dots,k_e} t_1^{k_1}\cdots t_e^{k_e} = \operatorname{Res}_{x_1,\dots,x_u} r(t_1,\dots,t_e,x_1,\dots,x_u)$$

for a rational series r, and if we define $\tilde{a}_{n_1,\dots,n_d} = a_{\lambda(n_1,\dots,n_d)}$ for $n_1,\dots,n_d \in \mathbb{N}$, then

$$\sum_{n_1,\dots,n_d\in\mathbb{N}} \tilde{a}_{n_1,\dots,n_d} \tau_1^{n_1}\cdots\tau_d^{n_d}$$

$$= \operatorname{Res}_{t_1,\ldots,t_e,x_1,\ldots,x_u} r(t_1,\ldots,t_e,x_1,\ldots,x_u) \prod_{i=1}^{e} t_i^{-1-\mu_i} \prod_{j=1}^{d} \frac{1}{1-\tau_j \prod_{i=1}^{e} t_i^{\lambda_{i,j}}},$$

for a term order for which the factors of the second product are expanded like geometric series, i.e., $\frac{1}{1-\tau_j \prod_{i=1}^{e} t_i^{\lambda_{i,j}}} = \sum_{n_j=0}^{\infty} \tau_j^{n_j} \prod_{i=1}^{e} t_i^{n_j \lambda_{i,j}}$.

This settles the case where the sequence $(\tilde{a}_{n_1,\ldots,n_d})_{n_1,\ldots,n_d \in \mathbb{N}}$ can be defined in terms of a binomial sum $(a_{k_1,\ldots,k_e})_{k_1,\ldots,k_e \in \mathbb{N}}$ whose support is $\mathbb{N}^e$. In general, $\tilde{a}$ is defined in terms of a binomial sum a whose support is $\mathbb{Z}^e$. Any such sequence a can be written as a finite sum of sequences whose support is restricted to one of the 2^e orthants of $\mathbb{Z}^e$, and each such summand can be mapped to $\mathbb{N}^e$ by replacing some variables of the respective generating function by their reciprocals. Once mapped to $\mathbb{N}^e$, it can be handled as indicated above.

6. Closure under indefinite sum follows from the identity

$$\sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_k\right) t^n = \frac{1}{1-t} \sum_{n\in\mathbb{N}} a_n t^n$$

Since we restrict to $n \geq 0$, there is no difference between the directed and standard sum here. ∎

The proof of the theorem can be easily translated into an algorithm which takes as input a binomial sum, specified by a symbolic expression that is composed according to the rules of Definition 5.80, and returns as output a rational function r and a term order such that the generating function of the binomial sum can be expressed as residue of r. Using reduction-based creative telescoping techniques, we can then find a D-finite description of this generating function. Note that we do not need the certificate in this case. Note also that the approach covers sums with natural boundaries as well as sums with non-natural boundaries, because non-natural boundaries can be encoded into the summand sequence using the functions from part 4 of Example 5.81.

Example 5.83

1. Let us prove $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ $(n \in \mathbb{N})$. For the indefinite sum $\sum_{k=0}^{m} \binom{n}{k}$ we have the generating function

$$\sum_{n,m\in\mathbb{N}} \left(\sum_{k=0}^{m} \binom{n}{k}\right) t_1^n t_2^m = \frac{1}{1-t_2} \frac{1}{1-(1+t_2)t_2}.$$

Setting $m = n$ in order to obtain the definite sum amounts to taking the diagonal, so

$$\sum_{n\in\mathbb{N}}\Bigl(\sum_{k=0}^{n}\binom{n}{k}\Bigr)t_1^n = \operatorname{diag}_{t_1,t_2}\frac{1}{1-t_2}\frac{1}{1-(1+t_2)t_1}$$
$$= \operatorname{Res}_{t_2}\frac{1}{t_2}\frac{1}{1-t_2}\frac{1}{1-(1+t_2)t_1/t_2}.$$

Creative telescoping finds that this residue is annihilated by $(1-2t_1)D_{t_1}-2$. As this operator also annihilates the generating function $1/(1-2t_1)$ of the right hand side and initial values on both sides match, the proof of the identity is complete.

2. Let us derive a differential equation for the generating function of the Apéry numbers $A_n = \sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2$. First observe that from

$$\sum_{n,k\in\mathbb{N}}\binom{n}{k}t_1^n t_2^k = \frac{1}{1-(1+t_2)t_1}$$

we get

$$\sum_{n,k\in\mathbb{N}}\binom{n+k}{k}t_1^n t_2^k = \frac{1}{1-(t_1+t_2)}.$$

The summand of the sum in question is a product of four binomials. It can be encoded by first forming

$$\sum_{n_1,n_2,n_3,n_4,k_1,k_2,k_3,k_4\in\mathbb{N}}\binom{n_1}{k_1}\binom{n_2}{k_2}\binom{n_3+k_3}{k_3}\binom{n_4+k_4}{k_4}t_1^{n_1}t_2^{n_2}t_3^{n_3}t_4^{n_4}t_5^{k_1}t_6^{k_2}t_7^{k_3}t_8^{k_4}$$

and then applying two diagonal operators by setting $n_1 = n_2 = n_3 = n_4$ and $k_1 = k_2 = k_3 = k_4$. The resulting expression is

$$\sum_{n,k\in\mathbb{N}}\binom{n}{k}^2\binom{n+k}{k}^2 t_1^n t_5^k = \operatorname{Res}_{t_2,t_3,t_4,t_6,t_7,t_8}\frac{1}{t_2t_3t_4t_6t_7t_8}\frac{1}{p}$$

where

$$p = \Bigl(1-\Bigl(1+\frac{t_5}{t_6t_7t_8}\Bigr)\frac{t_1}{t_2t_3t_4}\Bigr)(1-(1+t_6)t_2)(1-(t_3+t_7))(1-(t_4+t_8)).$$

It remains to take the indefinite sum over k, which corresponds to a multiplication with $1/(1-t_5)$, and to make the sum definite, which corresponds to taking another diagonal:

$$\sum_{n\in\mathbb{N}}A_n t_1^n = \operatorname{Res}_{t_2,t_3,t_4,t_5,t_6,t_7,t_8}\frac{1}{t_2t_3t_4t_5t_6t_7t_8}\frac{1}{1-t_5}\frac{1}{p(\frac{t_1}{t_5},t_2,\ldots,t_8)}.$$

Creative telescoping can find an annihilating operator for this sevenfold residue. □

As can be seen from these examples, the straightforward translation of a symbolic expression of a binomial sum into a residue expression for its generating function can lead to rational functions with a large number of variables. A large number of variables is disadvantageous because it can outweigh the complexity advantage that we obtain by not computing the certificates. More sophisticated translation algorithms, which we will not explain here, that try to minimize the number of variables arising in the rational functions are available. For example, in the case of the Apery numbers, these algorithms can find a rational function with four instead of eight variables (Exercise 22).

Exercises

1★. For a rational function $f \in C(x)$, let $g, h \in C(x)$ be the rational functions computed by Hermite reduction (Algorithm 5.1). Consider the function $R\colon C(x) \to C(x)$ which maps any rational function f to the corresponding h. Show that R is C-linear.

2★. Let V be a C-vector space and U be a subspace of V. Prove or disprove:

a. If R is a reduction for U with $R^2 = R$, then R is complete.
b. If R is a complete reduction for U, then $R^2 = R$.
c. If R is a reduction for U and $c \in C$, then $v \mapsto cR(v)$ is a reduction for U.
d. If R_1, R_2 are reductions for U, then $v \mapsto R_1(v) + R_2(v)$ is a reduction for U.
e. If R is a reduction for U, then $\ker R \cap \operatorname{im} R = \{0\}$.

3. In order to handle multivariate rational functions, we could iterate univariate Hermite reduction. For example, for a rational function $f \in C(t, x_1, x_2)$, we could first apply Hermite reduction with respect to x_1 to obtain g_1, h_1 with $f = (D_{x_1} \cdot g_1) + h_1$ and then apply Hermite reduction with respect to x_1 to h_1 to obtain g_2, h_2 with $h_1 = (D_{x_2} \cdot g_2) + h_2$, so that $f = (D_{x_1} \cdot g_1) + (D_{x_2} \cdot g_2) + h_2$. Is the map $R\colon C(t, x_1, x_2) \to C(t, x_1, x_2)$ which maps f to h_2 a reduction for the subspace $U = \{(D_{x_1} \cdot g_1) + (D_{x_2} \cdot g_2) : g_1, g_2 \in C(t, x_1, x_2)\}$? If so, is it confined or complete?

4★★. Let $p, q \in C[x_1, \dots, x_n]$. Prove or disprove:

a. If p is homogeneous of degree d, then $dp = \sum_{i=1}^n x_i (D_{x_i} \cdot p)$.
b. If $dp = \sum_{i=1}^n x_i (D_{x_i} \cdot p)$ for some d, then p is homogeneous of degree d.
c. If p and q are homogeneous, then

$$(\deg(p) - \deg(q))\frac{p}{q} = \sum_{i=1}^n x_i (D_{x_i} \cdot \frac{p}{q}).$$

d. If p and q are coprime and there is a constant d such that

$$d\frac{p}{q} = \sum_{i=1}^{n} x_i (D_{x_i} \cdot \frac{p}{q}),$$

then p and q are homogeneous and $\deg(p) - \deg(q) = d$.

5. Show that Algorithm 5.71 remains correct if line 2 is replaced by "If $k = 0$ or p and q are homogeneous and $n + \deg(p) \neq k \deg(q)$, return 0".
Hint: Use the results of the previous exercise.

6*. Prove the following facts:
a. For all $p, q \in C[x_1, \ldots, x_n]$ and $k \geq 2$ with $\langle D_{x_1} \cdot q, \ldots, D_{x_n} \cdot q\rangle = C[x_1, \ldots, x_n]$, there are $b_1, \ldots, b_n, c \in C[x_1, \ldots, x_n]$ such that $\frac{p}{q^k} = \sum_{i=1}^{n}(D_{x_i} \cdot \frac{b_n}{q^{k-1}}) + \frac{c}{q^{k-1}}$.
b. For $p, q \in C[x_1, \ldots, x_n]$ and $k \geq 2$ with $\langle D_{x_1} \cdot q, \ldots, D_{x_n} \cdot q\rangle \neq C[x_1, \ldots, x_n]$ the equation $\frac{p}{q^k} = \sum_{i=1}^{n}(D_{x_i} \cdot \frac{b_n}{q^{k-1}}) + \frac{c}{q^{k-1}}$ may not have a solution $(b_1, \ldots, b_n, c) \in C[x_1, \ldots, x_n]^{n+1}$.

7. Show that the output of Algorithm 5.71 depends on the choice of $b_1, \ldots, b_n$ in line 4.

8. For rational functions in a single variable, does the algorithm of Griffith-Dwork produce the same result as Hermite reduction?

9. Find telescopers for the following rational functions using reduction-based telescoping.
a. $\frac{x^4+y^4}{(x^3-tx^2y+y^3)^2}$ **b.** $\frac{x^4+y^4}{(x^3-x^2y+ty^3)^2}$ **c.** $\frac{x^7+y^7}{(x^3+ty^3)^3}$

10*. Show that reduction-based telescoping with Algorithm 5.71 does not terminate for $f = \frac{1}{t+x^3+x^2y}$.

11***. Let $u, v \in C[k]$ and consider the linear map $\varphi\colon C[k] \to C[k]$ defined by $\varphi(y) = u\sigma_k(y) - vy$.
a. Show that any set $B \subseteq C[k]$ such that for every $i \in \mathbb{N}$ there is exactly one $b \in B$ with $\deg_k(b) = i$ is a basis of $C[k]$.
b. Show that there exists a d such that for every $i \geq d$ the set $\operatorname{im}\varphi$ contains a polynomial of degree i.
c. Using the $d \in \mathbb{N}$ from part b, show that a subspace $W \subseteq C[k]$ with $C[k] = \operatorname{im}\varphi \oplus W$ can be computed with the help of Algorithm 2.56.

12. In the discussion following Theorem 5.77 we remarked that there is "no way" that $h - \tilde{h}$ can be the output of Algorithm 5.76 applied to $f - \tilde{f}$. Why is this so clear?

13*. Let $a, b \in \mathbb{N}$ be fixed, $f_{\text{ker}} = \Gamma(an + bk)$, and $P \subseteq C(n)[k]$ be a set of monic, irreducible, and pairwise not shift-equivalent polynomials containing $k + \frac{a}{b}n, \ldots, k + \frac{a+1}{b}n, \ldots, k + \frac{a+b-1}{b}n$. Derive an upper bound on the order of the minimal telescoper for f_{ker} by analyzing the hypergeometric terms h produced by Theorem 5.78 for $f = S_n^i \cdot \Gamma(an + bk)$ ($i \in \mathbb{N}$).

14⋆. Repeat the calculations of Example 5.79 using a P that contains $k+n+7$.

15. Evaluate once more the definite hypergeometric sums of Exercise 10 in Sect. 5.2, now using reduction-based telescoping.

16. Can it happen that Algorithm 5.76 applied to a kernel f_{ker} returns the kernel f_{ker} itself as output? Note that $f_{\mathrm{ker}} = (\frac{1}{1} + \frac{0}{v}) f_{\mathrm{ker}}$.

17⋆. Let $(u_k)_{k\in\mathbb{Z}}$ be any sequence and $q \in C \setminus \{0\}$. Prove the following facts about directed sums:

a. ${\sum'}_{k=a}^{b} u_k + {\sum'}_{k=b+1}^{c} u_k = {\sum'}_{k=a}^{c} u_k$ for all $a, b, c \in \mathbb{Z}$.

b. ${\sum'}_{k=a}^{b} q^k = \frac{q^a - q^{b+1}}{1-q}$ for all $a, b \in \mathbb{Z}$ and all $q \in C \setminus \{0\}$.

18. Let $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d \in \mathbb{Z}}$ be a binomial sum with $C = \mathbb{Q}$. Show that there is an integer $q \in \mathbb{Z}$ such that for all $n_1, \dots, n_d \in \mathbb{Z}$, the squarefree part of the denominator of $a_{n_1,\dots,n_d}$ divides q (in $\mathbb{Z}$).

19⋆. Show that $(n!)_{n\in\mathbb{N}}$ is not a binomial sum.

20. Express the generating functions of the following binomial sums as residues of rational functions:

a. $a_n = \sum_{k=0}^{n} \binom{n}{k}^2$ **b.** $b_n = \sum_{k=0}^{n} 2^k \binom{n+k}{k}$ **c.** $c_n = \sum_{k=0}^{n} \binom{3n}{2k}$.

21⋆. Consider rational functions as elements of $C_{\leq}((x_1, \dots, x_n))$ for a term order $\leq$ with $x_1 \geq x_i^j$ for $i = 2, \dots, n$ and all $j \in \mathbb{Z}$ (for example a lexicographic order).

a. Show that for all $p, q \in C(x_2, \dots, x_n)$ we have $\mathrm{Res}_{x_1} p/(1 - x_1 q) = 0$.

b. Show that there are $p, q \in C(x_2, \dots, x_n)$ such that $\mathrm{Res}_{x_n} p/(1 - x_1 q) \neq 0$.

c. Show that the residue $\mathrm{Res}_{x_1} r$ of any rational function $r \in C(x_1, \dots, x_n)$ is rational.

d. Show that the residue $\mathrm{Res}_{x_n} r$ of a rational function $r \in C(x_1, \dots, x_n)$ need not be rational.

22. With $A_n = \sum_k \binom{n}{k}^2 \binom{n+k}{k}^2$, show that

$$\sum_{n=0}^{\infty} A_n t^n = \mathrm{Res}_{x_1,x_2,x_3} \frac{1}{(1-x_1)(1-x_2)(1-x_3)x_1x_2x_3 - t(x_1 + x_2x_3 - x_1x_2x_3)}.$$

References

The first reduction-based algorithm for computing telescopers was given by Bostan, Chen, Chyzak and Li [86]. In that paper, repeated Hermite reduction was used for computing telescopers of rational functions in $C(t, x)$ in the differential case. In the following years, a bunch of papers appeared on reduction-based algorithms applicable to other domains. A first step was the extension to integration of hyperexponential functions by Bostan, Chen, Chyzak, Li and Xin [90]. This case is similar to the summation case for hypergeometric terms discussed in this section, which was introduced by Chen, Huang, Kauers and Li [138], where it was only shown that the reduction is complete. A year later, Huang showed that the reduction is also confined [242], which allowed her to obtain new upper and lower bounds on the order of telescopers for hypergeometric terms.

Reduction-based telescoping for rational functions in several variables using the Griffith-Dwork method was proposed by Bostan, Lairez and Salvy [91]. It is based on work of Griffith [224, 225] and Dwork [180, 181], who showed that under suitable assumptions their reduction is not only confined but also complete (cf. Thm. 1 in [91], credited to §4 of [224]). In Sect. 7.1 of [91], it is explained how to achieve the condition $\dim C[x_1, \ldots, x_n]/I < \infty$ by introducing a new variable. Alternative techniques to achieve the same goal avoiding the cost of a new variable are proposed by Lairez in [302]. Instead of translating a given integration problem into one for which Algorithm 5.71 succeeds, he proposes a hierarchy of stronger and stronger generalizations of Algorithm 5.71 with the feature that for every integrable rational function there is one reduction in the hierarchy that succeeds in integrating it.

The idea to solve summation problems by translating them into a residue computation goes back to Egoryshev [183], who proposed it as a method for hand-calculation. As such, it not only applies to binomial sums but also to sums that may involve Stirling numbers, for example. For binomial sums, Bostan, Lairez, and Salvy [95] turn this approach into an algorithm by combining it with reduction-based telescoping via Algorithm 5.71 and its generalization. Their paper also includes techniques not discussed here for keeping the number of variables in the rational function low.

Reduction-based telescoping algorithms have been formulated for some further classes of functions, including algebraic functions [140, 144], fuchsian D-finite functions [143], and general D-finite functions [97, 174, 438]. For the shift case, there is also a reduction-based algorithm for rational summands [145, 217].

Answers to Exercises

Section 1.1

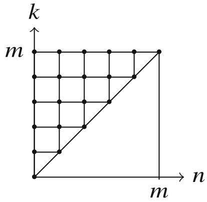
1. On the one hand it is not, because $B((x))$ and $B((x^{-1}))$ are defined as (disjoint) copies of a certain subset of the set $B^{\mathbb{Z}}$ of sequences. In this strict interpretation, $B((x))$ and $B((x^{-1}))$ have as much in common as $B((x))$ and $B((y))$, or $B((x))$ and $B((x-1))$, namely nothing. On the other hand, we can write a series $\sum_{n\in\mathbb{Z}} a_n x^{-n}$ in the form $\sum_{n\in\mathbb{Z}} a_{-n} x^n$, so that it looks like the elements of $B((x))$. Under this identification, the bilateral sequences that simultaneously are formal Laurent series in x and in x^{-1} are indeed the coefficient sequences of Laurent polynomials. With a similar identification, we might say that the intersection of $B((x))$ and $B((y))$ is B. In order to avoid confusion, we should refrain from giving an interpretation to the intersection of $B((x))$ and $B((x-1))$.

2. For $a(x) = \sum_{n=0}^{\infty} a_n x^n$, $b(x) = \sum_{n=0}^{\infty} b_n x^n$, $c(x) = \sum_{n=0}^{\infty} c_n x^n$ and every $m \in \mathbb{N}$ we have

$$\begin{aligned}
[x^m](a(x)b(x))c(x) &= \sum_{n=0}^{m}\Bigl(\sum_{k=0}^{n} a_k b_{n-k}\Bigr)c_{m-n} = \sum_{n=0}^{m}\sum_{k=0}^{n} a_k b_{n-k} c_{m-n}\\
&= \sum_{k=0}^{m}\sum_{n=k}^{m} a_k b_{n-k} c_{m-n} = \sum_{k=0}^{m}\sum_{n=0}^{m-k} a_k b_n c_{m-k-n}\\
&= \sum_{k=0}^{m} a_k\Bigl(\sum_{n=0}^{m-k} b_n c_{m-k-n}\Bigr) = [x^m]a(x)(b(x)c(x)),
\end{aligned}$$

as required. For the third step, observe that the summation ranges of the two double sums agree:

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1



3. Elements of $C[x][[y]]$ are power series in y whose coefficients are polynomials in x while elements of $C[[y]][x]$ are polynomials in x whose coefficients are power series in y. In both cases, we may write the elements in the form $\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} a_{n,k}x^k y^n$. The difference is that in the first case, we have $\forall\, n\ \exists\, k\ \forall\, \ell > k : a_{n,k} = 0$ while in the second case we have $\exists\, k\ \forall\, n\ \forall\, \ell > k : a_{n,k} = 0$. For example, $\sum_{n=0}^{\infty} x^n y^n$ belongs to $C[x][[y]]$ but not to $C[[y]][x]$.

4. a. $(1+x)^\alpha(1+x)^\beta = \sum_{n=0}^{\infty}\binom{\alpha}{n}x^n \sum_{n=0}^{\infty}\binom{\beta}{n}x^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{\alpha}{k}\binom{\beta}{n-k}x^n = \sum_{n=0}^{\infty}\binom{\alpha+\beta}{n}x^n = (1+x)^{\alpha+\beta}$. The third step is known as Vandermonde identity. **b.** $((1+x)^\alpha)' = \sum_{n=0}^{\infty}\binom{\alpha}{n+1}(n+1)x^n = \sum_{n=0}^{\infty}\alpha\binom{\alpha-1}{n}x^n$. The equality $\binom{\alpha}{n+1} = \frac{\alpha}{n+1}\binom{\alpha-1}{n}$ used in the second step follows immediately from the definition of the binomial coefficient. **c.**

$$\begin{aligned}
&\Big(\frac{((1+x)^\alpha)^\beta}{(1+x)^{\alpha\beta}}\Big)' \\
&= \frac{\beta((1+x)^\alpha)^{\beta-1}\alpha(1+x)^{\alpha-1}(1+x)^{\alpha\beta} - ((1+x)^\alpha)^\beta\alpha\beta(1+x)^{\alpha\beta-1}}{((1+x)^{\alpha\beta})^2} \\
&= \frac{\alpha\beta(1+x)^{\alpha\beta}((1+x)^\alpha)^\beta}{((1+x)^{\alpha\beta})^2}\Big(\frac{(1+x)^{\alpha-1}}{(1+x)^\alpha} - (1+x)^{-1}\Big) = 0.
\end{aligned}$$

This proves that the only possible nonzero coefficient of the quotient series is that of x^0. It remains to check that this coefficient is 1, which is easily seen by inspection.

5. a. follows from part a of Exercise 4; **b.** also follows from part a of Exercise 4, in combination with the fact that $(1+x)^0 = 1$; **c.** when $\alpha = p/q$ then $(1+x)^\alpha$ could be understood as an algebraic series satisfying the polynomial equation $y^q - (1+x)^p$, and by part c of Exercise 4, we have indeed $((1+x)^{p/q})^q = (1+x)^p$.

6. In order for a series $\sum_{n=0}^{\infty} b_n x^n$ to be a left inverse, we need to have $b_0 a_0 = 1$ and $\sum_{k=0}^{n} b_k a_{n-k} = 0$ for all $n > 0$. This forces us to set b_0 to the two-sided inverse of a_0, and to set $b_n = \sum_{k=0}^{n-1} b_k a_{n-k} b_0$ for $n > 0$. Note that we have used here that b_0 is also a right inverse of a_0. Analogously, $\sum_{n=0}^{\infty} b_n x^n$ is a right inverse if b_0 is the two-sided inverse of a_0 and $b_n = \sum_{k=0}^{n-1} b_0 a_k b_{n-k}$ for $n > 0$. To see that both recurrences have the same solution, show by induction that in either case, we obtain

$$b_n = (-1)^n \sum_{i_1+\cdots+i_n=n} b_0 a_{i_1} b_0 a_{i_2} b_0 \cdots b_0 a_{i_n} b_0$$

for all $n \in \mathbb{N}$.

7. $-1+2(x-1)-5(x-1)^2+13(x-1)^3-34(x-1)^4+89(x-1)^5+\cdots$ and $-1+2(x+1)-3(x+1)^2+5(x+1)^3-8(x+1)^4+13(x+1)^5+\cdots$, respectively.

8. There is no doubt that $f_n := \prod_{k=1}^n (1-x^k)$ is a well-defined element of $\mathbb{Z}[[x]]$ for every $n \in \mathbb{N}$. In fact, it is even an element of $\mathbb{Z}[x]$. We have $f_{n+1} - f_n = \prod_{k=1}^{n+1}(1-x^k) - \prod_{k=1}^n (1-x^k) = -x^{n+1} f_n$ for $n \in \mathbb{N}$, thus $\nu(f_{n+1} - f_n) > n$. Therefore the infinite sum $\sum_{n=0}^\infty (f_{n+1} - f_n)$ is well-defined in $\mathbb{Z}[[x]]$. It is natural to understand the infinite product as this series.

9. Write $f = \sum_{n=0}^\infty a_n x^{-n}$ and $g = x^k u$ for some $u \in C[[x]]$ with $u(0) \neq 0$. The composition ought to be $\sum_{n=0}^\infty a_n x^{-kn} u^{-n}$. We have to justify that this sum is well-defined. Indeed, since u has a multiplicative inverse in $C[[x]]$, all terms u^{-n} belong to $C[[x]]$. Moreover, since $k = \nu(g) < 0$ by assumption, $\nu(x^{-kn}u^{-n}) = -kn \geq n$ for all n. Therefore the sum is a valid power series.

10. Try an ansatz $f(x) = a_1 x + \cdots$. Since we must have $x^2 - xf(x) + x^2 f(x) - xf(x)^2 + f(x)^3 = (1-a_1)x^2 + \cdots = 0$, our only chance is to set $a_1 = 1$. Now substitute $f(x) = x(1+g(x))$ into the equation to obtain the new equation $x^2(-g(x) + x + 2xg(x) + 2xg(x)^2 + xg(x)^3) = 0$. After canceling x^2, we get an equation for $g(x)$ to which the implicit function theorem applies.

11. Because of $[x^0]f = 0$, we may write $f(x) = \sum_{n=1}^\infty a_n x^n$. Because of $[x^1]f \neq 0$, we have $a_1 \neq 0$. In order for a series $h(x) = \sum_{n=0}^\infty b_n x^n$ to be an outer inverse of f, we need to have $\sum_{n=0}^\infty b_n f(x)^n = x$. Comparing coefficients of x^0 and x^1 on both sides forces $b_0 = 0$ and $b_1 = 1/a_1$, respectively. For $n \geq 2$, comparing coefficients leads to $b_n = -\frac{1}{a_1} \sum_{k=0}^{n-1} b_k [x^n] f(x)^k$, and this recurrence has a unique solution. This shows the existence of the outer inverse.

If h is an outer inverse and g is an inner inverse of f, then $h(f(x)) = x$ and $f(g(x)) = x$ implies $h(x) = h(f(g(x))) = g(x)$, so the inverses agree.

12. Since differentiation is B-linear, it suffices to check the rules for single terms, which is an easy thing to do: We have $(x^n x^m)' = (x^{n+m})' = (n+m)x^{n+m-1} = nx^{n-1}x^m + mx^n x^{m-1}$ and $((x^n)^m)' = (x^{nm})' = nmx^{nm-1} = nmx^{n(m-1)+n-1} = (m(x^n)^{m-1})nx^{n-1}$ for all $n, m \in \mathbb{N}$.

13. $f(x) = x - \frac{1}{6}x^3 + \frac{1}{24}x^5 - \frac{61}{5040}x^7 + \frac{277}{72576}x^9 + \cdots$. There is also an explicit expression for the solution: $f(x) = 2\arctan(\tanh(x/2))$.

14. False. When z is not computable, then z is transcendental, because every algebraic number is computable. But for transcendental z, the field $\mathbb{Q}(z)$ is isomorphic to the rational function field $\mathbb{Q}(x)$, which is computable. Also when z is algebraic, the field $\mathbb{Q}(z)$ is computable.

15. "$\Rightarrow$": Let $c_0, \ldots, c_r \in C$ be such that $c_0 a_n + \cdots + c_r a_{n+r} = 0$ for all $n \in \mathbb{N}$. Then $\sum_{n=0}^\infty (c_0 a_n + \cdots + c_r a_{n+r}) x^n = 0$, which implies $c_0 \sum_{n=0}^\infty a_n x^n +$

$\cdots + c_r \sum_{n=0}^{\infty} a_{n+r}x^n = 0$. Now $\sum_{n=0}^{\infty} a_{n+i}x^n = x^{-i}(\sum_{n=0}^{\infty} a_n x^n - a_0 - a_1 x - \cdots - a_{i-1}x^{i-1})$ for every $i \in \mathbb{N}$, so for suitable polynomials $p_0, \dots, p_r$ we find the relation $c_0 f + \cdots + c_r x^{-r}(f - p_r) = 0$ for the series $f = \sum_{n=0}^{\infty} a_n x^n$. It follows that $f = (p_0 + x^{-1}p_1 + \cdots + x^{-r}p_r)/(c_0 + \cdots + c_r x^{-r})$ is rational.

"$\Leftarrow$": Let $p, q \in C[x]$ be such that $f = \sum_{n=0}^{\infty} a_n x^n = p/q$, and write $q = q_0 + q_1 x + \cdots + q_d x^d$. Then $qf = p$, and extracting the coefficient of x^n for $n > \max(\deg(p), \deg(q))$ gives the relation $q_0 a_n + q_1 a_{n-1} + \cdots + q_d a_{n-d} = 0$ for all $n > \max(\deg(p), \deg(q))$. Choosing $k \in \mathbb{N}$ sufficiently large, we obtain the recurrence $q_0 a_{n+k} + q_1 a_{n+k-1} + \cdots + q_d a_{n+k-d} = 0$, valid for all $n \geq 0$, which proves that $(a_n)_{n=0}^{\infty}$ is C-finite.

16. If the sequence were C-finite, then by the previous exercise, $\sum_{n=0}^{\infty} a_n x^n$ would be rational. Evaluating the rational function at $x = 10^{-1}$ would give a rational number, in contradiction to the irrationality of $\sqrt{2}$. Note that the rational function cannot have a pole at 10^{-1} because the series $\sum_{n=0}^{\infty} a_n 10^{-n}$ converges.

Alternative argument: the sequence $(a_n)_{n=0}^{\infty}$ has a finite image $\{0, \dots, 9\}$. Every C-finite sequence with finite image is ultimately periodic, because when there is a C-finite recurrence of order r, then each term of the sequence is uniquely determined by the preceding r terms, and when the sequence assumes only finitely many different terms, there can only be finitely many distinct runs of r consecutive terms. As soon as a run appears a second time, the sequence becomes periodic. Now if the sequence $(a_n)_{n=0}^{\infty}$ in the exercise were C-finite, it would be ultimately periodic, which again implies that $\sum_{n=0}^{\infty} a_n 10^{-n}$ would be rational.

17. If $p \in C[x][y]$ is a nonzero polynomial with $p(x, a(x)) = 0$, then $p(a^{-1}(x), x) = 0$.

18. No, and there are many ways to prove this. Here is one of them: if $\exp(x)$ were algebraic, there would be some $r \in \mathbb{N}$ and some rational functions $q_0, \dots, q_{r-1} \in C(x)$ such that $\exp(x)^r = \sum_{i=0}^{r-1} q_i(x)\exp(x)^i$. Among these r, choose one that is minimal. Differentiating on both sides gives $r\exp(x)^r = \sum_{i=0}^{r-1}(q_i'(x) + iq_i(x))\exp(x)^i$, and subtracting r times the first equation from the second leads to $0 = \sum_{i=0}^{r-1}(q_i'(x) + (i-r)q_i(x))\exp(x)^i$. By the assumption that r is minimal, it follows that $q_i'(x) = (i-r)q_i(x)$ for all i. But such rational functions q_i cannot have any poles or roots, because their multiplicities would be one less on the left than on the right. So the q_i must be constants. But then, $q_i'(x) = (r-i)q_i(x)$ even forces them to be zero, so our assumed equation for $\exp(x)$ collapses to $\exp(x)^r = 0$, which is obviously not a valid equation.

19. Yes, because $\arctan(x) = \frac{\mathrm{i}}{2}(\log(1 - \mathrm{i}x) - \log(1 + \mathrm{i}x))$.

20. If $\log(x)$ were algebraic, there would be some equation $\sum_{k=0}^{d} p_k(x)\log(x)^k = 0$ with $p_0, \dots, p_d \in C((x))$ and $p_d = 1$. Among those, select one where d is minimal. Differentiating this relation with respect to x gives $0 = \sum_{k=0}^{d} p_k'(x)\log(x)^k + kp_k(x)/x\log(x)^{k-1} = \sum_{k=0}^{d-1}(p_k'(x) + (k+1)p_{k+1}(x)/x)\log(x)^k$. This implies $p_k'(x) = -(k+1)p_{k+1}(x)/x$ for $k = 0, \dots, d-1$. For $k = d-1$, we find $p_k'(x) = -d/x$, which is impossible for $d \neq 0$, because the derivative of an element of $C((x))$ cannot contain the term $-dx^{-1}$. Since $d = 0$ is obviously not possible either, we can conclude that $\log(x)$ does not satisfy any polynomial equation with coefficients in $C((x))$.

21. For $f(x) = \int \frac{1}{\log x} dx$ we have $f'(x) = 1/\log(x)$, hence $\log(x) f'(x) = 1$, hence $\frac{1}{x} f'(x) + \log(x) f''(x) = 0$, hence $\frac{1}{x} f'(x) + f''(x)/f'(x) = 0$, hence $x = -f'(x)^2/f''(x)$, hence $1 = -\frac{2f'(x)f''(x)^2 - f'(x)^2 f'''(x)}{f''(x)^2}$. We have found that $f(x)$ satisfies the equation $f''(x)^2 + 2f'(x)f''(x)^2 - f'(x)^2 f'''(x) = 0$.

22. Write $\sum_{n=0}^{\infty} b_n x^n$ for the right hand side. A series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ is a solution of the equation iff we have $a_n - \sum_{k=0}^{\infty} a_k [x^n](\frac{x^2}{4x-1})^k = b_n$ for all $n \in \mathbb{N}$. Since $(\frac{x^2}{4x-1})^k = (-1)^k x^{2k} + \cdots$ for every $k \in \mathbb{N}$, we have $[x^n](\frac{x^2}{4x-1})^k = 0$ for all $n > k/2$. Therefore, $a_n = b_n + \sum_{k=0}^{\lfloor n/2 \rfloor} a_k [x^n](\frac{x^2}{4x-1})^k$ is a recurrence which uniquely determines each of the values $a_1, a_2, a_3, \ldots$ in terms of the previous ones. Since the first term $a_0 = 1$ is given, the claim follows.

The first few terms are $1 + x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + 132x^6 + 429x^7 + 1430x^8 + 4862x^9 + \cdots$. See Exercise 8 in Sect. 1.5 for more about this series.

Section 1.2

1. We need to show that f also satisfies a homogeneous differential equation with polynomial coefficients. A brutal way to do so is to differentiate the given inhomogeneous equation $d+1$ times, where d is the degree of q. Since $q^{(d+1)} = 0$, this will produce a homogeneous equation, at the cost of blowing up the order from r to $r+d+1$. A more gentle way is to differentiate the equation only once, obtaining a new linear differential equation of order $r+1$ with inhomogeneous part q'. Now q' times the original equation minus q times the new equation will be a homogeneous equation for f of order $r+1$.

2. arcsin and arccos are both annihilated by $(x^2-1)D^2 + xD$, the function arctan is annihilated by $(x^2+1)D^2 + 2xD$.

The tangent function is not D-finite. To see this, observe that $\tan'(z) = 1 + \tan(z)^2$ implies that for every $i \geq 1$ we have $\tan^{(i)}(z) = u_i(\tan(z))$ for some univariate polynomial u_i of degree $i+1$. Any potential differential equation $p_0(z)\tan(z) + \cdots + p_r(z)\tan^{(r)}(z) = 0$ with $p_r \neq 0$ would thus yield an algebraic equation of degree $r+1$ for tan. Since tan is a transcendental function, such an equation cannot exist.

3. $f^{(5)} = \frac{-16x^4 - 84x^3 - 99x^2 + 289x + 630}{(4x+5)^4} f + \frac{-8x^4 - 32x^3 - 12x^2 + 83x - 40}{(4x+5)^4} f'$.

4. H_n is annihilated by the operator $(n+1) - (2n+3)S + (n+2)S^2$. To see that 2^{2^n} is not D-finite, assume it were. Then there would be polynomials $p_0, \ldots, p_r$, with p_r not the zero polynomial, such that $p_0(n)2^{2^n} + \cdots + p_r(n)2^{2^{n+r}} = 0$ for all

$n \in \mathbb{N}$. Divide both sides by $n^{\deg p_r} 2^{2^{n+r}}$ and take the limit for $n \to \infty$. We get that the leading coefficient of p_r is zero, which is impossible.

5. It is easily checked by induction that $(\mathrm{e}^{\mathrm{e}^z})^{(i)} = q_i(\mathrm{e}^z)\mathrm{e}^{\mathrm{e}^z}$ for certain polynomials $q_i \in C[x]$ of degree i ($i \in \mathbb{N}$). Thus, if we had a differential equation $p_0(z)f(z) + \cdots + p_r(z)f^{(r)}(z) = 0$ with $p_r \neq 0$, we would have $p_0(z)q_0(\mathrm{e}^z) + \cdots + p_r(z)q_r(\mathrm{e}^z) = 0$, which is a nonzero algebraic equation for e^z. Since no such equation exists, the claim follows.

6. We have the recurrence $(n+1)f(n) - n\,f(n+1) = 0$ for all $n \in \mathbb{Z}$.

7. See Theorems 2.33 and 3.5.

8. "$\Rightarrow$" holds because $S = \{0, 1, \ldots, n_0\}$ is a finite set; "$\Leftarrow$" holds because every finite subset $S \subseteq \mathbb{N}$ has a maximal element, and $n_0 = \max S$ does the job.

9. "$\Rightarrow$": Suppose that $[f]$ is an equivalence class of sequences which satisfies the recurrence

$$p_0[f] + p_1 S[f] + \cdots + p_r S^r[f] = [0]$$

where $p_0, \ldots, p_r$ are polynomials, $p_r \neq 0$. By definition, this means that there exists a finite set $E \subseteq \mathbb{N}$ such that $p_0(n)f(n) + p_1(n)f(n+1) + \cdots + p_r(n)f(n+r) = 0$ for all $n \in \mathbb{N} \setminus E$. Therefore, with $q := \prod_{e \in E}(x - e)$, it follows that $q(n)p_0(n)f(n) + q(n)p_1(n)f(n+1) + \cdots + q(n)p_r(n)f(n+r) = 0$ for all $n \in \mathbb{N}$, thus f is D-finite. Since f is an arbitrary element of $[f]$, the argument applies to all elements of the class.

"$\Leftarrow$": If f is a D-finite sequence, say $p_0(n)f(n) + \cdots + p_r(n)f(n+r) = 0$ for all $n \in \mathbb{N}$, then we show that $p_0[f] + p_1 S[f] + \cdots + p_r S^r[f] = [0]$. Indeed, if g is any other sequence in $[f]$, say $f(n) = g(n)$ unless $n \in E$ for some fixed finite set $E \subseteq \mathbb{N}$, then for $i = 0, \ldots, r$ we have $f(n+i) = g(n+i)$ unless $n \in E \cup (E-1) \cup \cdots \cup (E-r)$, and therefore $p_0(n)g(n) + \cdots + p_r(n)g(n+r) = 0$ unless $n \in E \cup (E-1) \cup \cdots \cup (E-r)$. The claim follows.

10. "$\Rightarrow$": When f is D-finite, it satisfies a recurrence $S^r(f) = q_0 f + \cdots + q_{r-1}S^{r-1}(f)$ for some $q_0, \ldots, q_r \in C(x)$. For every $i \in \mathbb{N}$ we then have $S^{r+i}(f) = q_0(x+i)S^i(f) + \cdots + q_{r-1}(x+i)S^{r+i-1}(f)$, and it follows by induction that $S^{r+i}(f) \in C(x)f + \cdots + C(x)S^{r-1}(f)$. Since every element of $V(f)$ is a finite $C(x)$-linear combination of some terms $S^k(f)$ with $k \in \mathbb{N}$, it follows that $V(f) \subseteq C(x)f + \cdots + C(x)S^{r-1}(f)$, and thus $\dim_{C(x)} V(f) \leq r$. If r is minimal, then $\dim_{C(x)} V(f) = r$, because $\dim_{C(x)} V(f) < r$ would contradict the minimality of r.

"$\Leftarrow$": When $\dim_{C(x)} V(f) = r < \infty$ is finite, then any $r+1$ elements of $V(f)$ are linearly dependent over $C(x)$, in particular $f, S(f), \ldots, S^r(f)$. The coefficients of the linear dependence give rise to an equation of the required form.

11. False. For example, $f = \log(x)$ satisfies the differential equation $f' + xf'' = 0$ which has no term $p_0 f$, so if the statement were true, it would have to satisfy a first order differential equation $uf + vf' = 0$ with u, v polynomials. But this would imply that $\log(x) = -\frac{v(x)}{x\,u(x)}$ were a rational function, which is not the case.

12. False. For example, the sequence $f : \mathbb{N} \to C$ with $f(5) = 1$ and $f(n) = 0$ for $n \neq 5$ satisfies the "recurrence" $f(n+6) = 0$ for all $n \in \mathbb{N}$, but not the recurrence $f(n+5) = 0$ for all $n \in \mathbb{N}$. However, for germs or bilateral sequences the statement is true.

13. $PS(v)$. Observe the difference to the differential case, which originates from the fact that $S(uv) = S(u)S(v)$ while $(uv)' = u'v + uv'$.

14. We need that for all $M, L \in \ker\phi$ we have $M + L \in \ker\phi$ and for all $L \in \ker\phi$ and all $M \in C(x)[\phi]$ we have $ML \in \ker\phi$. The first property holds because $\phi(M + L) = (M + L) \cdot f = (M \cdot f) + (L \cdot f) = \phi(M) + \phi(L) = 0$. For the second, observe that $\phi(L) = 0$ and $M \cdot 0 = 0$ by the linearity of ∂.

15. One possibility is to write $L = \big((2x - 1) - (2x - 3)\partial\big)\big(1 + 2(1 - x)\partial\big)$.

16. Let $A(n, k)$ denote the left hand side of the first equation and $B(n, k)$ the left hand side of the second. Then

$$\begin{aligned} C(n, k) &:= A(n + 1, k) - (2(n + 1) + 3k)B(n, k + 1) \\ &= (n + 1 + k)f(n + 1, k) - (2(n + 1) + 3k)(4n + 5(k + 1))f(n, k + 1). \end{aligned}$$

By the second equation, the first term is equal to $(n + 1 + k)(4n + 5k)f(n, k)$. Furthermore, using the first equation, we can rewrite $(2n + 3k)C(n, k)$ to

$$\big((2n + 3k)(n + 1 + k)(4n + 5k) - (n + k)(2(n + 1) + 3k)(4n + 5(k + 1))\big)f(n, k).$$

Therefore, if $f(n, k)$ is a common solution of $A(n, k) = B(n, k) = 0$, then for all $n, k \in \mathbb{N}$ we have $(2n + 3k)(n + 1 + k)(4n + 5k) - (n + k)(2(n + 1) + 3k)(4n + 5(k + 1)) = 0$ or $f(n, k) = 0$. In other words, the germ of f is necessarily zero.

17. We need to show that the two given equations imply an equation containing only derivatives in y. Such an equation can indeed by constructed by suitably combining partial derivatives of the two given equations. For example, writing A and B for the left hand sides of the two given equations, we found

$$\begin{aligned} &\frac{x^2 - 4xy + 4y^2}{(y + 1)^2}\frac{\partial}{\partial x}A + \frac{x - 2y}{y + 1}\frac{\partial}{\partial y}A + \frac{x^2y - 2xy^2 + 2xy - x - 4y^2 + 4y + 2}{(y + 1)^2}A \\ &\qquad + \frac{8y^3 - x^3 + 6x^2y - 12xy^2}{(y + 1)^2}B \\ &= (2x^2y - 4xy^2 + 2x)f + (x^2 - 4y^2 + 2)\frac{\partial}{\partial y}f + (x - 2y)\frac{\partial^2}{\partial y^2}f. \end{aligned}$$

18. **a.** $f \sim f$ follows from $f = f$ with any choice of p. If $f \sim g$ via p, then the same p establishes also $g \sim f$. If $f \sim g$ via p and $g \sim h$ via q, then $f \sim h$ via pq.

b. "$\Rightarrow$" holds because a nonzero univariate polynomial p can have at most finitely many roots, so we can take $S = \{n \in \mathbb{N} : p(n) = 0\}$. "$\Leftarrow$" holds because when S is a finite set, then $\prod_{s\in S}(x - s)$ is a nonzero polynomial, which we can take as p.

19. No. Consider the sequence $f : \mathbb{N}^2 \to \mathbb{Q}$, $f(n, k) = (n + 1)^{-k}$. For every fixed n, it satisfied the recurrence $f(n, k) - (n+1)\, f(n, k+1) = 0$ and is therefore D-finite as univariate sequence in k, and for every fixed k, it satisfied the recurrence $(n + 1)^k f(n, k) - (n + 2)^k f(n, k + 1) = 0$ and is therefore D-finite as univariate sequence in n. Note that $(n+1)^k$ and $(n+2)^k$ are polynomials in n for every fixed k, even though they are not polynomials in n and k as would be required for bivariate D-finiteness. In fact, $f(n, k)$ is not bivariate D-finite. To show this, assume for the contrary that there are bivariate polynomials $p_0, \ldots, p_r$, $p_r \neq 0$, such that

$$\frac{p_0(n,k)}{(n+1)^k} + \cdots + \frac{p_r(n,k)}{(n+1+r)^k} = 0$$

for all $n, k \in \mathbb{N}$. Multiply by the common denominator and observing that $\gcd((x + i)^k, (x + j)^k) = 1$ whenever $i \neq j$, shows that for every $k \in \mathbb{N}$, the polynomial $(x + 1 + r)^k$ must divide $p_r(x, k)$. This is impossible because p_r is supposed to be a bivariate polynomial in both variables. Only for finitely many choices $k \in \mathbb{N}$ it can happen that $p_r(x, k)$ is identically zero, and for all other choices of k, the polynomial $p_r(x, k)$ is a nonzero polynomial of bounded degree in x, while the degree of $(x + 1 + r)^k$ is unbounded as k grows.

Section 1.4

1. **a.** counterexample: $f(n) = n$, $g(n) = 2n$; **b.** counterexample: $f(n) = 1 + (-1)^n$; $g(n) = 1$; **c.** proof: by assumption, there are $n_0 \in \mathbb{N}$ and $c_1, c_2 > 0$ such that for all $n \geq n_0$ we have $|f(n)| \leq c_1 g(n)$ and $|g(n)| \leq c_2 f(n)$. We may assume $c_1, c_2 > 1$. Then $|\max(f(n), g(n))| = \max(|f(n)|, |g(n)|) \leq c_1 g(n)$ and $|\max(f(n), g(n))| = \max(|f(n)|, |g(n)|) \leq c_2 f(n)$ for all $n \geq n_0$. Therefore, $|\max(f(n), g(n))| \leq \min(c_2 f(n), c_1 g(n)) \leq c \min(f(n), g(n))$ for $c = \max(c_1, c_2)$ and all $n \geq n_0$.

2. Let $\epsilon > 0$. It suffices to show that $\log(n)/n^\epsilon$ converges for $n \to \infty$. In fact, the we have that $\log(x)/x^\epsilon$ converges for $x \to \infty$ in the reals, since by the rule of l'Hospital the limit is equal to the limit of $\frac{1/x}{\epsilon x^{\epsilon-1}} = \epsilon^{-1} x^{-\epsilon}$, which is zero.

3. There is no final answer to this task.

4. No. The $O^{\sim}$ notation does not suppress every logarithmic term, but only contributions that are logarithmic compared to given argument. For example, $f(n) = O(\log(n)\log\log(n))$ implies $f(n) = O^{\sim}(\log(n))$ but not $f(n) = O^{\sim}(1)$.

5. **a.** In the first assumed inequality, set $n = ab$ and $m = b$, clear denominators and replace a, b by m, n, respectively. **b.** Wlog. $n \geq m$. From the first assumed inequality we have $M(n+m) \geq \frac{n+m}{n} M(n) = M(n) + \frac{m}{n} M(n)$. The second assumed inequality implies $M(m) = M(\frac{m}{n} n) \leq (\frac{m}{n})^2 M(n)$, so we get $M(n+m) \geq M(n) + \frac{n}{m} M(m) \geq M(n) + M(m)$, as claimed. **c.** By the second assumed inequality, we have $M(n) \leq n^2 M(1)$. **d.** By the first assumed inequality, we have $n \leq \frac{M(n)}{M(1)}$. **e.** For $c = 0$ the claim is obvious. For $c \geq 1$, the first assumed inequality gives $M(cn) \leq c\,M(n)$, which implies the claim.

6. By assumption, there exist $n_0 \in \mathbb{N}$ and $c > 0$ such that $|f(n)| \leq c\,M(n)$ for all $n \geq n_0$. Let $\tilde{c}$ be such that $\tilde{c} > c/\log(2)$ and $\tilde{c} > T(n)/M(n_0)$ for all $n = 0, \ldots, n_0$. We show by induction on n that $|T(n)| \leq \tilde{c}\,M(n)\log(n)$ for all $n \geq 0$. For $n \leq n_0$, this is true by the choice of $\tilde{c}$. Now let $n > n_0$ and assume the estimate holds for all numbers below n. Then $T(n) \leq 2T(n/2) + f(n) \leq 2\tilde{c}\,M(n/2)\log(n/2) + c\,M(n) \leq 2\tilde{c}\,M(n/2)(\log(n) - \log(2)) + c\,M(n) \leq \tilde{c}\,M(n)\log(n) + (c - \tilde{c}\log(2))\,M(n) \leq \tilde{c}\,M(n)\log(n)$, where we have used the assumption $\tilde{c} > c/\log(2)$ in the last step and the estimate $2\,M(n/2) \leq M(n)$ in the step before.

7. If k is even, we have $p^k = (p^{k/2})^2$, and if k is odd, we have $p^k = p(p^{(k-1)/2})^2$. If we apply this scheme recursively and take into account that $\deg(p^k) = kn$, we get a cost $T(n,k)$ which satisfies $T(n,k) \leq T(n,k/2) + c\,M(kn)$, for some $c > 0$. Let $\tilde{c} > 2c$, and suppose that k is such that $T(n,m) \leq \tilde{c}\,M(mn)$ for all $m < k$. Then $T(n,k) \leq T(n,k/2) + c\,M(kn) \leq \tilde{c}\,M(nk/2) + c\,M(kn) \leq (\tilde{c}/2 + c)\,M(kn) \leq \tilde{c}\,M(kn)$, which implies that $T(n,k) \leq \tilde{c}\,M(kn)$. The claim follows.

8. Both operations can be performed with $O(M_{\mathbb{Z}}(n)\log(n))$ bit operations on input numbers with numerators and denominators of n bits. The runtime is dominated by the cost for recognizing common factors that may have to be canceled.

9. When m is not a prime, say $m = uv$ for two proper divisors $u, v \in \mathbb{Z}$, then $[u][v] = [m] = [0]$ in $\mathbb{Z}_m$ while $[u] \neq [0]$ and $[v] \neq [0]$. The elements $[u]$ and $[v]$ cannot have multiplicative inverses, because if there were a $[p]$ such that $[p][u] = [1]$ then $[p][u][v] = [0]$ and $[p][u][v] = [v]$ would imply $[0] = [v]$, in contradiction to v being a proper divisor of m.

10. The modular solutions are $(7,7)$, $(9,9)$, and $(10,10)$, respectively. The Chinese remainder theorem merges them into the solution $(2100, 2100)$ modulo 4199. Rational reconstruction finally yields the solution vector $x = (1/2, 1/2)$. In the second set of primes, 23 turns out to be an unlucky modulus, because the matrix A is singular modulo 23. In $\mathbb{Z}_{23}^2$ the solution set of the system consists of all vectors $(9,0) + \alpha(6,1)$ with $\alpha \in \mathbb{Z}_{23}$, and there is no way to tell to which of them we should apply the Chinese remainder theorem.

11. Arithmetic complexity only counts additions, subtractions, multiplications, divisions, and equality tests in the coefficient domain, none of which are required for the operations in question. From the perspective of arithmetic complexity, these operations are therefore for free. Of course, they still consume some time in actual implementations. How much time exactly, this depends mostly on implementation details, but it should be fair to assume in most cases that the time is negligible.

12. The problem can be reduced to multiplication of polynomials in one variable as follows. Replace y by x^{2d_x+1} in the two input polynomials to obtain two polynomials in $C[x]$ of degree at most $d_x + d_y(2d_x + 1) = \mathrm{O}(d_x d_y)$. This does not cost any arithmetic operations. Their product can be computed within the required bound. In the resulting polynomial, replace each term x^u by $x^{\mathrm{rem}(u,2d_x+1)} y^{\mathrm{quo}(u,2d_x+1)}$. It is easy to see that the resulting polynomial is the product pq. This trick is known as *Kronecker substitution* and also applies in other situations.

13. Computing the derivative of a polynomial of degree n requires $\mathrm{O}(n)$ operations in R.

14. Compute $p(0), p(1), p(2), \dots, p(n) \in C$. According to part 4, this can be done using $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations. Now compute a polynomial q of degree n with $q(1) = p(0), q(2) = p(1), \dots, q(n+1) = p(n)$. According to part 5, this can also be done using $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations. By construction, the polynomial $p(x+1) - q(x)$ has at least $n+1$ roots but its degree is at most n. It is therefore the zero polynomial. Thus $q(x)$ is the desired result.

The assumption that C has characteristic zero was used when we assumed that the field elements $0, 1, \dots, n$ are pairwise distinct.

15. This is known as *Horner's rule:* Write the polynomial $p(x) = p_0 + p_1 x + \cdots + p_n x^n$ in the form $p(x) = p_0 + x(p_1 + x(p_2 + x(p_3 + x(\cdots))))$. Replacing x by c in the expression on the right evaluates to $p(c)$, at the cost of n multiplications and at most n additions.

16. "$\Rightarrow$": If p is squarefree, it is the product of pairwise coprime irreducible polynomials. Apply induction on the number of factors. If p itself is irreducible, then $\gcd(p, p') = 1$ because $\deg(p') = \deg(p) - 1 < \deg(p)$. For the induction step, let $u, v \in C[x]\setminus C$ be two coprime polynomials with $\gcd(u, u') = \gcd(v, v') = 1$. Suppose that $g := \gcd(uv, (uv)') \neq 1$ and consider an irreducible factor q of g. Since u, v are coprime, q must be either a factor of u or of v. If it is a factor of u, then $q \mid (uv)' = u'v + uv'$ implies $q \mid u'v$, and since q is then not a factor of v, it follows that $q \mid u'$, in contradiction to the assumption $\gcd(u, u') = 1$. The case when q is a factor of v is analogous.

This direction is not true in positive characteristic. For example, in $\mathbb{Z}_3[x]$ we have $\gcd(x^3 + 1, 3x^2) = x^3 + 1 \neq 0$ although $x^3 + 1$ is squarefree. We have used the assumption about the characteristic in the step $\deg(p') = \deg(p) - 1$. "$\Leftarrow$": If p is not squarefree, then we have $p = q^2 u$ for some $q \in C[x] \setminus C$ and some $u \in C[x]$. Because of $p' = 2qq'u + q^2u' = q(2q'u + qu')$, we see that $q \mid \gcd(p, p')$, so $\gcd(p, p') \neq 1$. This direction also works for fields with positive characteristic.

17. No. For example, $\nu_{(x+1)(x+2)}((x+1)(x+2)) = 1 \neq 0+0 = \nu_{(x+1)(x+2)}(x+1) + \nu_{(x+1)(x+2)}(x+2)$.

18. We can write $r = (x-\xi)^{\nu_\xi(r)} q$ for some $q \in C(x)$ which has neither a root nor a pole at ξ and which therefore amounts to a formal power series in $C[[x-\xi]]$ which starts with exponent 0. Therefore, the series associated to r in $C((x-\xi))$ starts with exponent $\nu_\xi(r)$, as claimed.

19. Compute the square free decomposition (Part 1 of Theorem 1.25) of the numerator and denominator of u. We have a perfect square if and only if all exponents are even.

20. **a.** $(x^2+2x+3)^2$; **b.** $(x^2+5x+2)(x^2+6x+3)$; **c.** $(x+4)(x+12)(x+21)(x+29)$; **d.** $(x+5)(x+21)(x+22)(x+38)$; **e.** x^4+4x^3-8x-1; **f.** $(x^2-(\sqrt{2}-2)x-\sqrt{2}-1)(x^2+(2+\sqrt{2})x+\sqrt{2}-1)$; **g.** x^4+4x^3-8x-1; **h.** $(x^2+2x-\sqrt{5}-2)(x^2+2x+\sqrt{5}-2)$.

21. **a.** True: if $u, v \in C[x]$ are such that $p(x+c) = u(x)v(x)$ then $p(x) = u(x-c)v(x-c)$, and since $\deg u(x) = \deg u(x-c)$ and $\deg v(x) = \deg v(x-c)$, the claim follows. **b.** False: $p = x^5 + 1 \in \mathbb{Q}[x]$ is irreducible but $D(p) = 5x^4$ is not.

22. Since $\alpha > 1$, we will have $n^\alpha > n$ when n is large. Divide each matrix into $n^{\alpha-1}$ blocks of size $n \times n$. The matrix product can be obtained by multiplying corresponding blocks together and adding the results. The multiplications consume $n^{\alpha-1}\,\mathrm{O}(n^\omega)$ operations and the additions cost $n^{\alpha-1}n^2$ operations.

Section 1.5

1. Write $p_i = \sum_{j=0}^d p_{i,j}x^j$ for $i = 0, \dots, r$ with undetermined coefficients $p_{i,j}$. Then for every $n \in \mathbb{N}$, the expression $p_0(n)a_n + \cdots + p_r(n)a_{n+r}$ is a linear combination of the undetermined coefficients $p_{i,j}$. Setting these linear combinations to zero for $n = 0, \dots, N-r$ gives a homogeneous system of linear equations with $(r+1)(d+1)$ variables and $N-r+1$ equations. The solution space of such a system has dimension at least $(r+1)(d+1)-(N-r+1)$.

2. Algorithm 1.33 finds that $V_{2,2}$ is a vector space of dimension 1 generated by $(4x+8x^2, 6-6x-6x^2, -3+2x+x^2)$. Since the sequence satisfies by assumption a recurrence of order 2 and degree 2 and $V_{2,2}$ must contain the coefficient vector of this recurrence, it follows that the sequence in fact satisfies the recurrence $(4n+8n^2)a_n + (6-6n-6n^2)a_{n+1} + (-3+2n+n^2)a_{n+2} = 0$ for all $n \in \mathbb{N}$. Together with the initial values, the recurrence can be used to calculate recursively any other term a_n, in particular a_{20}.

3. Guessing finds the candidate

$$(-8-16n)a_n+(32+20n)a_{n+1}+(-22-8n)a_{n+2}+(4+n)a_{n+3}=0.$$

To show that this recurrence is correct, let b_n denote the left hand side. We know from the solution of the previous problem that $(4n+8n^2)a_n+(6-6n-6n^2)a_{n+1}+(-3+2n+n^2)a_{n+2}=0$ holds for all $n\in\mathbb{N}$. Replacing n by $n+1$ gives $(12+20n+8n^2)a_{n+1}+(-6-18n-6n^2)a_{n+2}+(4n+n^2)a_{n+3}=0$. Subtracting this equation from nb_n gives

$$(-8n-16n^2)a_n+(-12+12n+12n^2)a_{n+1}+(6-4n-2n^2)a_{n+2},$$

which is the -2-fold of the recurrence for a_n, and therefore equal to zero for all $n\in\mathbb{N}$. Thus $nb_n=0$ for all $n\in\mathbb{N}$, and therefore $b_n=0$ for all $n\geq 1$. Direct calculation confirms that also $b_0=0$, and this completes the proof.

4. First calculate the first 50 or so coefficients of the function's series expansion at the origin. The coefficient sequence starts with $2,\frac{1}{2},\frac{11}{8},\frac{11}{48},\dots$. Use this data to guess a linear differential equation. One of several possible results is the equation

$$\begin{aligned}
&(216x^6+1080x^5+2232x^4+2344x^3+1216x^2+224x-16)f^{(3)}(x)\\
&+(-216x^5-1080x^4-2088x^3-2152x^2-1232x-304)f''(x)\\
&+(-486x^7-2592x^6-5886x^5-7002x^4-4098x^3-460x^2\\
&+712x+308)f'(x)\\
&+(-243x^6-1053x^5-1890x^4-1044x^3+858x^2+1180x+352)f(x)=0
\end{aligned}$$

Finally, prove that $\exp(x\sqrt{1+x})+\frac{1}{\sqrt{1+x}}$ satisfies this equation by plugging it into the left hand side and simplifying it.

5. 1. Obviously $V_{r,d}\subseteq V_{r,d+1}$, so we are done if we can find at least $\dim_C V_{r,d}-\dim_C V_{r,d-1}$ many linearly independent elements of $V_{r,d+1}$ which do not already belong to $V_{r,d}$. Indeed, there are $\dim_C V_{r,d}-\dim_C V_{r,d-1}$ many linearly independent elements of $V_{r,d}$ which do not belong to $V_{r,d-1}$. Multiplying them by x gives as many linearly independent elements of $V_{r,d+1}$ not belonging to $V_{r,d}$.

2. The same argument applies with two minor differences: first, $V_{r,d}\subseteq C[x]^{r+1}$ and $V_{r+1,d}\subseteq C[x]^{r+2}$ have different ambient spaces, so we don't have $V_{r,d}\subseteq V_{r+1,d}$ in the strict sense, but we still have $V_{r,d}\hookrightarrow V_{r+1,d}$ in a natural way, and this is good enough. The second difference is that instead of multiplying the $\dim_C V_{r+1,d}-\dim_C V_{r,d}$ many linearly independent solutions of order exactly r by x, we have to differentiate or shift the corresponding equations to obtain the desired linearly independent equations of order exactly $r+1$.

6. Since guessing with, say, 100 terms does not find any candidate equations, it follows that no equation exists.

7. Read r horizontally and d vertically:

5	0	5	10	15	21	27
4	0	4	8	12	17	22
3	0	3	6	9	13	17
2	0	2	4	6	9	12
1	0	1	2	3	5	7
0	0	0	0	0	1	2
	0	1	2	3	4	5

8. $x(4x-1)f''(x)+2(5x-1)f'(x)+2f(x)=0$; $(n+2)a_{n+1}-2(2n+1)a_n=0$.

9. The recurrence is $(n+1-n_0)a_{n+1}-a_n=0$ $(n \in \mathbb{N})$. In order to find it, long runs of zeros are of no use because they only contribute trivial equations $0=0$ to the linear system. The recurrence can be recovered from $a_0, a_1, \dots, a_{n_0+2}$.

10. Using the first 60 terms of the series, on can easily find $(x-1)^2(x+1)^2f^6 + 3(x-1)^3(x+1)^2f^4+2(x-1)(x+1)f^3+3(x-1)^4(x+1)^2f^2-6(x-1)^2(x+1)f + x(x^3-2x^2-x+3)(x^3-x^2+1)=0$. If desired, the guess can be verified by plugging the given closed form into the right hand side and checking that it simplifies to zero.

11. $\sum_{k=1}^{n}\big(\sum_{i=1}^{k}\frac{1}{i}\big)^2 = 2n-(2n+1)\sum_{k=1}^{n}\frac{1}{k}+(n+1)\big(\sum_{k=1}^{n}\frac{1}{k}\big)^2.$

12. $(-3m+2n+1)f_{n,m}+(-m-2n-3)f_{n+1,m}+(m+1)f_{n+1,m+1}=0$

13. With the modular data we can find that the recurrence $(57+55n)a_n+(1+n)a_{n+1}=0$ holds in $\mathbb{Z}_{59}$. This recurrence is normalized and rational reconstruction applied to its coefficients yields $(-2-4n)a_n+(1+n)a_{n+1}=0$. Together with the initial value $a_0=1$, this recurrence produces the terms $1, 2, 6, 20, 70, 252$, so a good guess would be $a_5=252$. The fact that the recurrence produces integers rather than rational numbers with denominators is a good sign that the recurrence is correct.

14. For $p=5$ the sequence is obviously D-finite. Let p be some other prime. By Fermat's little theorem, $5^{p-1}\equiv 1 \bmod p$ for every prime p. Therefore, $5^{(n+(p-1))^3}=5^{n^3+3(p-1)n^2+3(p-1)^2n+(p-1)^3}=5^{n^3}(5^{p-1})^{3n^2+3(p-1)n+(p-1)^2}\equiv 5^{n^3} \bmod p$. Therefore we have the recurrence $a_{n+p}-a_n=0$, and this shows that the sequence is D-finite modulo every fixed prime p.

To see that it is not D-finite as a sequence in $\mathbb{Z}$, suppose it were. Let $p_0(n)a_n+\dots+p_r(n)a_{n+r}=0$ be a recurrence with polynomial coefficients. We may assume that the polynomials have integer coefficients and p_0 is not the zero polynomial. After dividing by 5^{n^3}, we can conclude that $p_0(n)=-5^{3n}\big(p_1(n)5^{3n^2+1}+\dots+p_r(n)5^{3n^2r+3n(r^2-1)+r^3}\big)$. Since p_0 is not the zero polynomial, the left hand side is nonzero for infinitely many $n \in \mathbb{N}$. Since the p_i have integer coefficients, the expression in the parentheses on the right evaluates to an integer for every $n \in \mathbb{N}$. It follows that $|p_0(n)| \geq 5^{3n}$ for infinitely many $n \in \mathbb{N}$, and this is impossible when p_0 is a polynomial.

15. It is better to go $\mathbb{Q}(t) \xrightarrow{mod} \mathbb{Z}_p(t) \xrightarrow{eval} \mathbb{Z}_p$, because in the other version, setting t to some rational number might require long-integer arithmetic, while setting t to an element of $\mathbb{Z}_p$ is cheaper.

16. The minimum of $(r+1)(\alpha + \frac{\beta}{r-\gamma} + 2)$ as a function of r is near $r = \gamma \pm \sqrt{\frac{\beta(1+\gamma)}{2+\alpha}}$.

17. The longest integer coefficient appearing in the polynomials $p_0(x), \ldots, p_6(x)$ is 114722421028178616762921041 10. The longest integer coefficient appearing in the polynomials $p_0(x-3), \ldots, p_6(x-3)$ is 173669097734852884188. We see that shifting a polynomial in general affects the size of the coefficients. This is not surprising because $\sigma^k(\sum_{j=0}^d c_j x^j) = \sum_{j=0}^d c_j (x+k)^j = \sum_{i=0}^d (\sum_j c_j \binom{j}{i} k^{j-i}) x^i$, and the binomials can easily get large. For every recurrence $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ of a D-finite sequence $(a_n)_{n=0}^\infty$ there is some $i \in \mathbb{Z}$ for which the lengths of the integers in $p_0(x-i), \ldots, p_r(x-i)$ is minimal. Experience suggests that $i \approx r/2$ is a good choice.

18. The minimal order recurrence has order 5 and degree 29, and the longest integer coefficient appearing in it is 531680254438102058017090988569142604.

19. The minimal order differential equation has order 10 and degree 32, and the longest integer coefficient appearing in it is 2918736877790848 5469100409561478612622719488.

20. If f is even, then f' is odd, and if f is odd, then f' is even. Consider a differential equation $\sum_{i=0}^r \sum_{j=0}^d a_{i,j} x^j f^{(i)} = 0$. Substituting x by $-x$ and using that f is even, we obtain the differential equation $\sum_{i=0}^r \sum_{j=0}^d (-1)^{i+j} a_{i,j} x^j f^{(i)} = 0$. Combining the two equations gives $\sum_{i=0}^r \sum_{j=0}^d (1-(-1)^{i+j}) a_{i,j} x^j f^{(i)} = 0$, so in the ansatz for a differential equation, we may assume without loss of generality that $a_{i,j} = 0$ for every pair (i,j) such that $i+j$ is odd. We then have only $(r+1)(d+1)/2$ variables, so we only need $N > (r+1)(d+1)/2$ equations to get an overdetermined system. Note however that in order to really obtain so many equations, we must know the coefficients $[x^n]f$ for $n = 0, 2, 4, \ldots, 2N+r$, because the other coefficients just lead to the equation $0 = 0$. Kauers and Verron observe that in the recurrence case, deleting zeros from the data not only leads to smaller linear systems but also to a small saving of data terms [274].

Section 1.6

1. The minimal polynomial is $3x(3451x^2+55779)y^2-24(10611x^2+13160)y+x(139967x^2+315840)$. It leads to the approximate value 1.11943 for $x=.9$, the correct value being 1.11977 to five decimal digits. The best Padé approximant is $\frac{x(69049x^4-717780x^2+922320)}{15(9675x^4-58100x^2+61488)}$ and leads to the approximate value 1.11545.

2. The recurrence produces $\frac{17134746796394397578197126258344694159960928414479 36}{92887648508199215840875025868167}$, its distance to the true value $16^{16}=18446744073709551616$ is less than 0.02. For a proof that $(n^n)_{n=0}^{\infty}$ is not D-finite, see [210].

3. Let V be the vector space generated by $\{x^i b_j : j=1,\dots,r, i=0,\dots,d-\deg^\delta b_j\}$.

To show that $V\subseteq M_{\sigma,d}$, let $p\in V$, say $p=p_1b_1+\cdots+p_rb_r$ for some $p_1,\dots,p_r$ with $\deg p_j\leq d-\deg^\delta b_j$. Then $\deg^\delta p\leq\max_{j=1}^r(\deg p_j+\deg^\delta b_j)\leq d$. Furthermore, by $\operatorname{ord}_f b_i\geq\sigma$ we have $\operatorname{ord}_f p\geq\sigma$. It follows that $p\in M_{\sigma,d}$.

To show that $V\supseteq M_{\sigma,d}$, let $p\in M_{\sigma,d}$. Since $\{b_1,\dots,b_r\}$ is a σ-basis, there exist $q_1,\dots,q_r\in C[x]$ with $\deg q_j+\deg^\delta b_i\leq d$ and $p=q_1b_1+\cdots+q_rb_r$. As each q_j is a C-linear combination of $x^0,\dots,x^{d-\deg^\delta b_j}$, it follows that $p\in V$.

4. $(8-28x+48x^2-52x^3+24x^4)D_x^2+(-8+90x-162x^2+84x^3)D_x+(16+2x-82x^2+153x^3-135x^4+54x^5)$

5. $(9x^2-17x+8)D_x^2-2(8x^3+x^2-17x+7)D_x+(16x^3+25x^2-65x-12)$ and $(x^2-x)D_x^2+(-2x^2+2x+2)D_x+(x^2-x-4)$.

6. No. If $\{b_1,\dots,b_r\}$ is a σ-basis for f with respect to δ, and if the indexing of the basis elements is so that $\deg^\delta b_1\leq\cdots\leq\deg^\delta b_r$, then also $\{b_1,b_1+b_2,b_3,\dots,b_r\}$ is a σ-basis for f with respect to δ.

7. The answer depends heavily on how exactly the algorithms are being implemented, as well as on characteristics of the chosen computer algebra system and maybe even on the physical hardware on which the experiments are carried out. The author's implementation in Sage uses a constant around 64.

8. The idea is to take a D-finite series $f\in C[[x]]$ and a non-D-finite series $g\in C[[x]]$ and let Algorithm 1.45 search for possible differential equations satisfied by $f+x^kg$, for some suitably chosen fixed $k\in\mathbb{N}$. Then during the first iterations the algorithm will discover the differential equation for f and maintain it in the basis until it sees some of the terms of g. At this iteration it will have to modify the basis element corresponding to the true equation for f.

To be specific, take $f=\sqrt{1-x}$, which satisfies an equation of order one and degree one, and $g=\exp(\exp(x)-1)$, which is not D-finite. Let $h=f+x^8g$ and apply the algorithm to (h,h'), $\delta=(0,0)$. The development of $\deg b_1,\deg b_2,\operatorname{ord}b_1,\operatorname{ord}b_2$ is then as follows.

σ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\deg b_1$	0	1	1	2	3	4	5	6	6	6	6	6	6	7	7	8
$\deg b_2$	0	0	1	1	1	1	1	1	2	3	4	5	6	6	7	7
$\operatorname{ord} b_1$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\operatorname{ord} b_2$	0	1	2	7	7	7	7	7	8	9	10	11	12	13	14	15

9. This is true when B is the identity matrix, $\det(I_r) = 1 = x^0$, and it remains true whenever Algorithm 1.45 updates B, because any such update is either a multiplication of a column by x or the addition of a constant multiple of one column to another.

10. The rational reconstruction problem can be solved by Hermite-Padé approximation. Searching for $p, q \in C[x]$ such that $p \equiv aq \bmod m$ is equivalent to searching for $p, q, r \in C[x]$ such that $p + aq + rm = 0$. For a solution with $\deg(p) < k$ and $\deg(q) \leq n - k$ we will have $\deg(r) < n - k \leq n$. Such a solution will also satisfy $p + aq + rm = \mathrm{O}(x^{2n})$, so (p, q, r) will be an element of $M_{2n,n}$ for $f = (1, a, m)$ and $\delta = (n - k, k, 0)$, so a solution will appear in a σ-basis for f and δ. According to Theorem 1.51, the computation of such a basis costs $\mathrm{O}(\mathrm{M}(n)\log(n))$ operations in C (using $r = 3$ and $\sigma = 2n$ and absorbing multiplicative constants).

11. Apply Algorithms 1.45 or 1.50 to $f = (f_1, f_2)$ with $f_1 = -1$ and $f_2 = 1 + 5x + 4x^2 + 3x^3 + 7x^4 + 36x^5 + 84x^6 + 142x^7 + 231x^8 + 497x^9$, and with $\delta = (4, 0)$. The resulting σ-basis with $\sigma = 10$ contains a vector $b = (p, q)$ with $p = 1 + 3x - 5x^2$ and $q = 1 - 2x + x^2 - 5x^4 + x^6$. By construction, we have $qf_2 - p = \mathrm{O}(x^{10})$, so $f_2 = \frac{p}{q} + \mathrm{O}(x^{10})$, as desired.

12. In Algorithm 1.45: replace the definition of c_i in line 5 by $(b_i \cdot f)_s$, the sth term of the sequence $b_i \cdot f$. Replace line 11 by $b_\ell = (x - s)b_\ell$.

In Algorithm 1.50: replace $(x^{-\tilde{\sigma}} B f^T) \bmod x^{\sigma - \tilde{\sigma}}$ in line 4 by $S_x^{\tilde{\sigma}} \cdot (Bf^T)$, i.e., calculate the first terms of the sequences in Bf^T and discard the first $\tilde{\sigma}$ many of them. Replace line 6 by "Return $B'|_{x=x+\tilde{\sigma}} B$".

In order to save the substitution $x = x + \tilde{\sigma}$, we could also use an additional input parameter $\rho \in \mathbb{N}$ in both algorithms, then set $b_\ell = (x - s - \rho)b_\ell$ in line 11 of Algorithm 1.45 and recurse with $\rho + \tilde{\sigma}$ instead of ρ in line 5 of Algorithm 1.50.

Section 2.1

1. $$\frac{2762289897(1407285 \text{ digits suppressed})8222075419}{2843860936(966223 \text{ digits suppressed})0000000000}$$

2. In order to find the solutions of a recurrence $p_0(n)a_n+\dots+p_r(n)a_{n+r} = b_n$ for given polynomials $p_0, \dots, p_r \in C[x]$ and given initial values $a_0, \dots, a_r$, it suffices to replace line 8 by

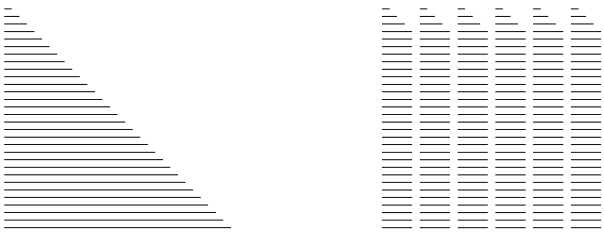
$$\text{Set } (A_0, \dots, A_{r-1}) = (A_1, \dots, A_{r-1}, b_{n-r} - \frac{1}{p_r(n-r)} \sum\nolimits_{i=0}^{r-1} p_i(n-r)A_i).$$

3. Suppose we have $q_0(n)b_n + \dots + q_s(n)b_{n+s} = 0$ and $p_0(n)a_n + \dots + p_r(n)a_{n+r} = b_n$ for all $n \in \mathbb{N}$. Then

$$\begin{pmatrix} b_{n+1} \\ \vdots \\ b_{n+s} \\ a_{n+1} \\ \vdots \\ a_{n+r} \end{pmatrix} = \begin{pmatrix} U(n) & 0 \\ V & W(n) \end{pmatrix} \begin{pmatrix} b_n \\ \vdots \\ b_{n+s-1} \\ a_n \\ \vdots \\ a_{n+r-1} \end{pmatrix}$$

where $U(x) \in C(x)^{s\times s}$ is the companion matrix for the recurrence for $(b_n)_{n=0}^\infty$ and $W(x) \in C(x)^{r\times r}$ is the companion matrix for the homogeneous part of the recurrence for $(a_n)_{n=0}^\infty$ and $V \in C^{r\times s}$ is the matrix which has a 1 in the lower left corner and all other entries are zero.

4. Not necessarily. The use of homomorphic images is striking whenever the length of the integers in the output is significantly smaller than the length of the integers in intermediate expressions. In the application at hand, we must expect that the final result a_N is the largest integer arising in the computation. In fact, it is even likely that the use of homomorphic images slows down the computation. To see why, note that computing in $\mathbb{Z}$ benefits from the fact that smaller terms are shorter. This effect gets lost when the terms are computed modulo several primes:



5. The recurrence for $(b_n)_{n=0}^\infty$ has polynomial coefficients of degree 3 while the recurrence for $(a_n)_{n=0}^\infty$ has polynomial coefficients of degree 1. Because of the degree difference, each iteration of the algorithm must be expected to take about three times longer for $(b_n)_{n=0}^\infty$ than for $(a_n)_{n=0}^\infty$. Therefore, although we need only half as many iterations using $(b_n)_{n=0}^{\infty}$, this computation would still take about $3/2 = 1.5$ times as long as the computation with the recurrence for $(a_n)_{n=0}^{\infty}$.

6. Computation in the ring $\mathbb{Z}_{10^{20}}$ leads to the result 39807042248059253307.

7. We have $P(n)P(n)^* = \begin{pmatrix} I_{r-1} & \bar{u} \\ u & s \end{pmatrix}$ with $u = -(\frac{p_1(n)}{p_r(n)}, \dots, \frac{p_{r-1}(n)}{p_r(n)})$ and $s = u\bar{u} + |\frac{p_0(n)}{p_r(n)}|^2$. The characteristic polynomial of this matrix is

$$\begin{aligned}\begin{vmatrix} (1-x)I_{r-1} & \bar{u} \\ u & s-x \end{vmatrix} &= (1-x)^{r-1} \begin{vmatrix} I_{r-1} & (1-x)^{-1}\bar{u} \\ u & s-x \end{vmatrix} \\ &= (1-x)^{r-1} \begin{vmatrix} I_{r-1} & (1-x)^{-1}\bar{u} \\ 0 & s-x-u\bar{u}(1-x)^{-1} \end{vmatrix} \\ &= (1-x)^{r-2}((s-x)(1-x)-u\bar{u}),\end{aligned}$$

so its eigenvalues are 1 and $\frac{1}{2}((s+1) \pm \sqrt{(1-s)^2 + 4u\bar{u}})$. Since the squares of the singular values of $P(n)$ are the eigenvalues of $P(n)P(n)^*$, the claim follows.

8. For $N \in \mathbb{N}$, we have $\sum_{n=N}^{\infty} \frac{(2n)!!}{(2n+1)!!}(\frac{1}{2})^n \leq \sum_{n=N}^{\infty}(\frac{1}{2})^n = 2^{1-N}$. Therefore, as soon as $2^{1-N} \leq 10^{-100}$, an exact computation will get the first 100 decimal digits right. A possible choice is $N = 334$. We have to ensure that the error $(\epsilon_2, \epsilon_1, \epsilon_0)$ is so small that the error ϵ_N for the Nth computed term is less than 10^{-100}. If $\sigma_{\max}(n)$ denotes the largest singular value of the companion matrix $P(n)$, we have $|\epsilon_N| \leq \|(\epsilon_{N-2}, \epsilon_{N-1}, \epsilon_N)\| \leq \prod_{n=1}^{N-2} \sigma_{\max}(n) \|(\epsilon_0, \epsilon_1, \epsilon_2)\|$, so we are safe if $\|(\epsilon_0, \epsilon_1, \epsilon_2)\| \leq 10^{-100} / \prod_{n=1}^{N-2} \sigma_{\max}(n)$. For estimating the expression on the right, we can use calculus and the formula from the previous exercise to find the n for which $\sigma_{\max}(n)$ is maximal. It turns out to be $n = 1$. Since $\sigma_{\max}(1) \leq 5.793$, we are guaranteed to get 100 correct digits if $\|(\epsilon_0, \epsilon_1, \epsilon_2)\| \leq 10^{-100}/5.793^{332} \leq 5.2003 \cdot 10^{-354}$. This bound is pessimistic, though. In fact, an initial accuracy of about 10^{-200} would already suffice.

9. Because of $\sigma_{\max} = \lim_{n\to\infty} \sigma_{\max}(n)$, there exists $n_0 \in \mathbb{N}$ such that $|\sigma_{\max}(n) - \sigma_{\max}| \leq \epsilon$ for all $n \geq n_0$. Then $\sigma_{\max}(n) \leq \sigma_{\max} + \epsilon$ for these n, so $\|(a_n, \dots, a_{n-r+1})\| \leq \|P(n-1)\cdots P(n_0)(a_{n_0}, \dots, a_{n_0+r-1})\| \leq \sigma_{\max}(n-1)\cdots\sigma_{\max}(n_0)\|(a_{n_0}, \dots, a_{n_0+r-1})\| \leq (\sigma_{\max}+\epsilon)^{n-n_0}\|(a_{n_0}, \dots, a_{n_0+r-1})\|$ for all $n \geq n_0$. We can thus take $c = \|(a_{n_0}, \dots, a_{n_0+r-1})\|/(\sigma_{\max}+\epsilon)^{n_0}$.

10. **a.** By the triangle inequality: $|(\xi_1+\xi_2) - (\bar{\xi}_1+\bar{\xi}_2)| = |(\xi_1-\bar{\xi}_1)+(\xi_2-\bar{\xi}_2)| \leq |\xi_1-\bar{\xi}_1|+|\xi_2-\bar{\xi}_2| < \epsilon_1+\epsilon_2$. **b.** $|\xi_1\xi_2-\bar{\xi}_1\bar{\xi}_2| = |\xi_1\xi_2-\xi_1\bar{\xi}_2+\xi_1\bar{\xi}_2-\bar{\xi}_1\bar{\xi}_2| \leq |\xi_1||\xi_2-\bar{\xi}_2| + |\xi_1-\bar{\xi}_1||\bar{\xi}_2| = |\xi_1-\bar{\xi}_1+\bar{\xi}_1||\xi_2-\bar{\xi}_2| + |\xi_1-\bar{\xi}_1||\bar{\xi}_2| \leq (\epsilon_1+|\bar{\xi}_1|)\epsilon_2+\epsilon_1|\bar{\xi}_2|$.

11. There are positive constants c, d such that for every $n \in \mathbb{N}$ the entries of each matrix $P(n)$ are rational numbers whose numerators and denominators are bounded by cn^d. The coefficients in the product $P(n)P(n-1)\cdots P(0)$ then have numerators and denominators that cannot exceed $c^n n^{nd}$. This implies that a D-finite sequence can asymptotically grow at most as fast as $n^{O(n)} = 2^{O(n \log n)}$. The sequence 2^{n^2} grows faster.

12. For the purpose of this exercise, we can ignore the dependence on r and d. Then the cost of line 5 is $O^{\sim}(s) = O(N^{\alpha})$ while the cost of line 6 is $O^{\sim}(t) = O^{\sim}(N^{1-\alpha})$. The overall cost is therefore $O^{\sim}(N^{\max(\alpha,1-\alpha)})$, and hence the choice $\alpha = 1/2$ is optimal.

13. The leading coefficient polynomial of the recurrence is $2n + 5$, which has no zeros in $\mathbb{Z}$ but does have a zero in every finite field $\mathbb{Z}_p$. Indeed, for $p = 1091$ we have $2 \cdot 543 + 5 = 1091$. Therefore, for every $n \in 541 + 1091\mathbb{Z}$, the value of a_n cannot be computed via the recurrence. On the other hand, for $p = 9223372036854775783$ we have undetermined terms only for $n \in 4611686018427387887 + p\mathbb{Z}$, and so there is no problematic index in the range $0, 1, \ldots, 10000000000000$.

Section 2.2

1. In $\mathbb{Q}^{\mathbb{N}}$, the solution space is generated by the sequences $1, 0, 0, 0, \ldots$ and $0, 1, 0, 0, \ldots$. The solution space in $\mathbb{Q}^{\mathbb{Z}}$ contains only the zero sequence.

2. For example

n	0	1	2	3	4	5	6	7	8	$\cdots$
	1	$-\frac{3}{22}$	$-\frac{1}{11}$	$\frac{3}{22}$	$-\frac{3}{11}$	0	$-\frac{25}{11}$	$-\frac{45}{11}$	$-\frac{885}{77}$	$\cdots$
	0	0	0	0	0	1	4	$\frac{57}{5}$	$\frac{876}{35}$	$\cdots$

3. Because of $p_r(s_m) = 0$, any sequence $(a_n)_{n=0}^{\infty}$ with $a_{s_m+r} = 1$ and $a_n = 0$ for all $n < s_m + r$ satisfied the recurrence for all $n \leq s_m + r$. Since s_m is the largest integer root of p_r, the recurrence can be used to extend these initial values to all $n > s_m + r$.

4. Let $s_1, \ldots, s_m \in \mathbb{N}$ be pairwise distinct, and consider the recurrence

$$(n - s_1)(n - s_2) \cdots (n - s_m)a_n - (n - s_1)(n - s_2) \cdots (n - s_m)a_{n+r} = 0.$$

This recurrence has a set of $m + r$ linearly independent solutions: r solutions of the form $(\delta_{n \bmod r,i})_{n=0}^{\infty}$ $(i = 0, \ldots, r - 1)$ as well as the m solutions $(\delta_{n,s_i})_{n=0}^{\infty}$ $(i = 1, \ldots, m)$.

5. False. The recurrence $(n + 3)a_n - (n + 3)a_{n+1} = 0$ has only constant solutions in $C^{\mathbb{N}}$, thus $\dim_C V_{\mathbb{N}} = 1$, but its solution space in $C^{\mathbb{Z}}$ is generated by the following two sequences, so $\dim_C V_{\mathbb{Z}} = 2 > 1$.

n	-5	-3	-2	-1	0	1	$\cdots$
	1	1	1	0	0	0	$\cdots$
	0	0	0	1	1	1	$\cdots$

6. True. The reasoning about partial solutions right before Theorem 2.16 applied to the backwards recurrence shows that when there are $\dim_C V_{\mathbb{N}}$ linearly independent solutions which are valid for all $n \geq 0$, then there are at least as many which are valid for all $n \geq N$, for every $N \in \mathbb{Z}$. The claim follows.

Note however that it is in general not true that every solution in $C^{\mathbb{N}}$ can be extended to a solution in $C^{\mathbb{Z}}$. For example, the recurrence $a_{n+1} - (n+2)a_n = 0$ has a solution $(a_n)_{n=0}^{\infty}$ with $a_0 = 1$, but an attempt to extend this solution towards the left forces $(-1+2)a_{-1} = a_0 \Rightarrow a_{-1} = -1$ and then $(-2+2)a_{-2} = a_{-1}$, which is a false statement no matter how we choose a_{-2}.

7. The space consists of all constant multiples of the sequence

n	0	1	2	3	4	5	6	7	8	$\cdots$
	0	0	1	0	0	$\frac{1}{5}$	$\frac{23}{40}$	$\frac{89}{100}$	$\frac{1277}{960}$	$\cdots$

8. The full solution space is generated by the sequences $(\delta_{n,3})_{n=0}^{\infty}$ and $(\delta_{n,5})_{n=0}^{\infty}$. Only constant multiples of $(\delta_{n,5})_{n=0}^{\infty}$ are robust solutions.

9. The leading and trailing coefficients of the deformed recurrence have no integer roots. Therefore, if a solution has a run of r consecutive zero terms, this run continues indefinitely to the left and to the right, and thus the solution can only be the zero solution.

10. It is clear that the sum of two solutions is a solution. Suppose that $a(z)$ is a solution, and let $c(z)$ be an element of $\mathfrak{M}_1$. Then for all z we have

$$
\begin{aligned}
& p_0(z)a(z) + p_1(z)a(z+1) + \cdots + p_r(z)a(z+r) = 0 \\
\Longrightarrow\quad & c(z)\big(p_0(z)a(z) + p_1(z)a(z+1) + \cdots + p_r(z)a(z+r)\big) = 0 \\
\Longrightarrow\quad & p_0(z)c(z)a(z) + p_1(z)c(z)a(z+1) + \cdots + p_r(z)c(z)a(z+r) = 0 \\
\Longrightarrow\quad & p_0(z)c(z)a(z) + p_1(z)c(z+1)a(z+1) + \cdots + p_r(z)c(z+r)a(z+r) = 0,
\end{aligned}
$$

so the product $c(z)a(z)$ is also a solution of the recurrence.

11. Let $p_0, \ldots, p_r \in C[x]$ be the coefficient polynomials of the recurrence, and let $N \in \mathbb{N}$ be such that neither p_0 nor p_r has an integer root greater than N.

To see that the dimension is at most r, let $[(a_n^{(1)})_{n=0}^{\infty}], \ldots, [(a_n^{(r+1)})_{n=0}^{\infty}]$ be elements of V. We show that they are linearly independent. Without loss of generality, we can assume the representatives $(a_n^{(1)})_{n=0}^{\infty}, \ldots, (a_n^{(r+1)})_{n=0}^{\infty}$ to be such that they satisfy the recurrence for all $n \geq N$. By the choice of N, every solution

$(a_n)_{n=N}^{\infty}$ of the recurrence is uniquely determined by the r values $a_N, \dots, a_{N+r-1}$. Therefore, the sequences $(a_n^{(1)})_{n=0}^{\infty}, \dots, (a_n^{(r+1)})_{n=0}^{\infty}$ belong to a vector space of dimension at most r. Hence they are linearly dependent.

To see that the dimension is at least r, let $(a_n^{(i)})_{n=N}^{\infty}$ $(i = 1, \dots, r)$ be the sequence solutions of the recurrence defined by $a_{n+j}^{(i)} = \delta_{i,j}$ for $i, j = 1, \dots, r$. We show that the equivalence classes $[(a_n^{(i)})_{n=N}^{\infty}]$ $(i = 1, \dots, r)$ are linearly independent. If $c_1, \dots, c_r$ are such that $c_1[(a_n^{(1)})] + \cdots + c_r[(a_n^{(r)})] = 0$ then there exists an $n_0 \geq N$ such that $c_1 a_n^{(1)} + \cdots + c_r a_n^{(r)} = 0$ for all $n \geq n_0$. By the choice of N, we can apply the recurrence backwards and see that $c_1 a_n^{(1)} + \cdots + c_r a_n^{(r)} = 0$ even holds for all $n \geq N$. Since the sequences $(a_n^{(i)})_{n=N}^{\infty}$ are linearly independent, this implies that $c_1 = \cdots = c_r = 0$.

12. First note that when p is the characteristic of F, we have $u(n) = u(n + p)$ for every $u \in F[x]$ and every $n \in \mathbb{N}$. **a.** By the observation just made, the subsequences $(a_{pn+i})_{n=0}^{\infty}$ for fixed $i \in \mathbb{N}$ satisfy recurrence equations with constant coefficients. A recurrence with constant coefficients in a finite field can only have solutions that are ultimately periodic, because for any $n \in \mathbb{N}$, there are only $|F|^r$ different possibilities for the vector $(b_n, \dots, b_{n+r-1})$, and the components of this vector (together with the recurrence) determine the next value. Hence there are $n_1, n_2 \in \mathbb{N}$ such that $n_1 \neq n_2$ and $(b_{n_1}, \dots, b_{n_1+r-1}) = (b_{n_2}, \dots, b_{n_2+r-1})$, and for any such n_1, n_2, we have $b_{n+|n_1-n_2|} = b_n$ for all $n \in \mathbb{N}$. Since the interlacing of ultimately periodic sequences is ultimately periodic, the claim follows. **b.** For $F = \mathbb{Z}_2$, consider the recurrence $(n^2 + n)a_n = 0$ of order 0. Note that $x^2 + x \in F[x]$ is not the zero polynomial, yet $n^2 + n = 0$ for all $n \in \mathbb{N}$. Therefore, the solution space of the recurrence is the space $F^{\mathbb{N}}$ of all sequences. In particular, there are non-periodic solutions.

13. **a.** False. For example, $\sigma(f) - 2f = 1 - x$ has the solution $f = x$ in $K = C(x)$ while $\sigma(f) - 2f = 0$ has no solution in $C(x)$. **b.** False. For example, $\sigma(f) - f = 0$ has the solution $f = 1$ in $K = C(x)$ while $\sigma(f) - f = 1/x$ has no solution in $C(x)$. **c.** True. Take any $f \in K$ and set $g = p_0 f + \cdots + p_r \sigma^r(f)$.

14. It is clear by definition that C is contained in the constant field. Conversely, let $r \in C(x)$ be such that $r(x + 1) = r(x)$. It is clear that r cannot have any poles, because a rational function can have at most finitely many poles, and so if there were any, there would be a pole $\alpha \in \bar{C}$ such that $\alpha + k$ is not a pole for any $k \in \mathbb{N}$. But then α cannot also be a pole of $r(x+1)$, in contradiction to $r(x+1) = r(x)$. It is also clear that r cannot have any roots, because $r(x + 1) = r(x)$ implies $\frac{1}{r(x+1)} = \frac{1}{r(x)}$, so we can employ the same argument as before. Since we have shown that $r \in C(x)$ has neither roots nor poles, it follows that $r \in C$, as claimed.

15. It is clear by definition that C is contained in the constant field. Furthermore, because of $\sigma(x^2) = \sigma(x)^2 = (-x)^2 = x^2$, it follows that $C(x^2)$ is contained in the constant field. Conversely, consider an arbitrary constant $c \in C(x) \setminus C(x^2)$. Write $c = p(x)/q(x)$ for some $p, q \in C[x]$, and write $p(x) = p_0(x^2) + x p_1(x^2)$ and $q(x) = q_0(x^2) + x q_1(x^2)$ for some polynomials $p_0, p_1, q_0, q_1 \in C[x]$. Since c is a constant, $\sigma(c) = c$ implies $p(-x)q(x) - p(x)q(-x) = 0$. Then

$$\begin{aligned} 0 &= (p_0(x^2) - xp_1(x^2))(q_0(x^2) + xq_1(x^2)) \\ &\quad - (p_0(x^2) + xp_1(x^2))(q_0(x^2) - xq_1(x^2)) \\ &= 2x(p_0(x^2)q_1(x^2) - p_1(x^2)q_0(x^2)), \end{aligned}$$

then $p_0(x^2) = p_1(x^2)q_0(x^2)/q_1(x^2)$. Therefore

$$c = \frac{p(x)}{q(x)} = \frac{p_1(x^2)(q_0(x^2) + xq_1(x^2))}{q_1(x^2)(q_0(x^2) + xq_1(x^2))} = \frac{p_1(x^2)}{q_1(x^2)} \in C(x^2),$$

as required.

16. We have $\sigma(x^p - x) = (x+1)^p - (x+1) = x^p - x$. This implies "$\supseteq$". For "$\subseteq$", observe that the set $\{(x+1)^k - x^k \mid k \in \mathbb{Z} \setminus p\mathbb{Z}\}$ is linearly independent over $\mathbb{Z}_p$, because the polynomials $(x+1)^k - x^k = kx^{k-1} + \cdots$ with $k \nmid p$ have distinct leading terms.

17. If $I \neq \{0\}$, then I contains some nonzero element $a \in R$. This element can be written as $a_1 g_1 + \cdots + a_n g_n$ for certain $a_1, \ldots, a_n \in K$, not all zero. Let i be such that $a_i \neq 0$. Then $a \in I$ implies $a_i^{-1} g_i a = g_i \in I$. Since I is closed under σ, it follows that $g_1, \ldots, g_m \in I$, and thus finally $g_1 + \cdots + g_m = 1 \in I$.

18. **a.** Since R is a K-vector space of dimension m, it suffices to show that $g_0, \ldots, g_{m-1}$ are linearly independent. This is the case because $(g_0, \ldots, g_{m-1}) = D(1, \phi^x, \ldots, \phi^{(m-1)x})$ where $F = ((\phi^{ij}))_{i,j=0}^{m-1} \in K^{m \times m}$ is the matrix of the discrete Fourier transform, which is a Vandermonde matrix and therefore invertible. **b.** We have $\sum_{i=0}^{m-1} g_i = \frac{1}{m} \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \phi^{ij} (\phi^x)^j = \frac{1}{m} \sum_{j=0}^{m-1} (\sum_{i=0}^{m-1} \phi^{ij})(\phi^x)^j$, and since $\sum_{i=0}^{m-1} \phi^{i0} = m$ and $\sum_{i=0}^{m-1} \phi^{ij} = \frac{\phi^{jm}-1}{\phi^j - 1} = 0$ for $j \neq 0$, the claim follows. **c.** $g_i g_j = \frac{1}{m^2} \sum_{u=0}^{m-1} \sum_{v=0}^{m-1} \phi^{iu+jv} (\phi^x)^{u+v} = \frac{1}{m^2} \sum_{v=0}^{m-1} \sum_{u=0}^{m-1} \phi^{iu+j(v-u)} (\phi^x)^v = \frac{1}{m^2} \sum_{v=0}^{m-1} m\delta_{i,j} \phi^{jv} (\phi^x)^v = \delta_{i,j} g_i$. **d.** follows directly from the definition of g_i and the fact that ϕ is an mth root of unity.

19. The direction "$\Rightarrow$" is obvious. We show "$\Leftarrow$". Write $Y = (y_1, \ldots, y_r) \in K^r$. If $W(y_1, \ldots, y_r) = 0$, then the vectors $Y, \sigma(Y), \ldots, \sigma^{r-1}(Y)$ are linearly dependent over K, say $a_0 Y + \cdots + a_{r-1}\sigma^{r-1}(Y) = 0$ for some $a_0, \ldots, a_{r-1} \in K$, not all zero. Thus $y_1, \ldots, y_r \in K$ are solutions of a linear recurrence of order at most $r-1$. The claim follows by Theorem 2.26.

20. $(x-1)x^2 f(x+3) - (x-1)(x^3 + 6x^2 + 4x + 1) f(x+2) + (3x^3 + 6x^2 - 3x - 2)(x+1) f(x+1) - 2x(x+1)^3 f(x) = 0$.

Section 2.3

1. Obvious.

2. It is clear that $\binom{un+v}{sn+t}$ is D-finite for all nonnegative integers u, v, s, t. For the general case, it suffices to consider the case $a_n := \binom{\lfloor(un+v)/d\rfloor}{\lfloor(sn+t)/d\rfloor}$ for some positive integers u, v, s, t, d. Clearly, for every $i = 0, \ldots, d-1$, the subsequence $(a_{dn+i})_{n=0}^{\infty}$ is D-finite, because $\lfloor(u(dn+i)+v)/d\rfloor = un + \lfloor(ui+v)/d\rfloor$ and likewise for the lower argument. The interlacing of the D-finite sequences $(a_{dn+i})_{n=0}^{\infty}$ $(i = 0, \ldots, d-1)$ gives the sequence $(a_n)_{n=0}^{\infty}$, which is therefore also D-finite by Theorem 2.32.

3. The sequence $(n)_{n=0}^{\infty}$ satisfies the recurrence $nf(n+1) - (n+1)f(n) = 0$ $(n \in \mathbb{N})$. From here, we can compute recurrence equations for the subsequences $(\lfloor\frac{n}{3}\rfloor)_{n=0}^{\infty}$, $(\lfloor\frac{n+2}{6}\rfloor)_{n=0}^{\infty}$, $(\lfloor\frac{n+4}{6}\rfloor)_{n=0}^{\infty}$, $(\lfloor\frac{n}{2}\rfloor)_{n=0}^{\infty}$, $(\lfloor\frac{n+3}{6}\rfloor)_{n=0}^{\infty}$ by Theorem 2.32. Then by Theorem 2.30, we can construct a recurrence which has all these sequences as solutions, in particular the left hand side and the right hand side of the claimed identity. The recurrence turns out to be $f(n+7) - f(n+6) - f(n+1) + f(n) = 0$. Therefore, it suffices to check the identity $n = 0, \ldots, 6$. Since it holds for these points, the recurrence implies that it holds for all $n \in \mathbb{N}$.

4. The right hand side satisfies the recurrence $2(n+1)f(n+1) - (2n+1)f(n) = 0$. If we write the left hand side as $n! \sum_{k=0}^{n} \frac{1}{(n-k)!}(-\frac{1}{4})^k \frac{(2k)!}{k!^3}$, the sum has the form of a convolution. Starting from the recurrence equations $(n+1)f(n+1) - f(n) = 0$ and $2(n+1)^2 f(n+1) - (2n+1)f(n) = 0$ satisfied by $\frac{1}{n!}$ and $(-\frac{1}{4})^n \frac{(2n)!}{n!^3}$, respectively, we can construct the corresponding differential equations, then a differential equation for their product, and then the corresponding recurrence of this differential equation. This yields the recurrence $2(n+1)^2 f(n+1) - (2n+1)f(n) = 0$ for the sum $\sum_{k=0}^{n} \frac{1}{(n-k)!}(-\frac{1}{4})^k \frac{(2k)!}{k!^3}$. Finally, from this recurrence and the recurrence $f(n+1) - (n+1)f(n) = 0$ for $n!$, we can find the recurrence $2(n+1)f(n+1) - (2n+1)f(n) = 0$ for the left hand side.

The recurrence for left hand side and right hand side agree, and they have order one and no positive integers as singularities. Therefore, it suffices to compare the values of both sides for $n = 0$, which is 1, and the recurrences imply inductively that both sides agree for all $n \in \mathbb{N}$.

5. With $a(x) = \sum_{n=0}^{\infty} a_n x^n$, $b(x) = \sum_{n=0}^{\infty} b_n x^n$, $c(x) = \sum_{n=0}^{\infty} c_n x^n$, we have $d_n = [x^n]a(x)b(x)c(x)$. By Theorem 2.33, $a(x), b(x), c(x)$ are D-finite. By Theorem 3.25, it follows that $a(x)b(x)c(x)$ is D-finite. The claim follows by Theorem 3.5.

6. For every $i \in \mathbb{N}$, a suitable polynomial multiple of b_{n+i} can be expressed as a linear combination with polynomial coefficients of the r terms $a_n, \ldots, a_{n+r-1}$. Therefore, the $r+1$ terms $b_n, \ldots, b_{n+r}$ must satisfy a linear relation with polynomial coefficients.

7. Consider the difference $c_n = b_n - a_n$. By assumption, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ we have $c_n = 0$. Therefore, $(c_n)_{n=0}^{\infty}$ is D-finite; it satisfies for example the (degenerate) recurrence $c_{n+n_0+1} = 0$ for all $n \in \mathbb{N}$. Since $b_n = a_n + c_n$ is the sum of two D-finite sequences, it is D-finite.

8. Because of $a_{n+i}a_{n+j} = a_{n+j}a_{n+i}$, the ansatz for the recurrence can be rewritten to a polynomial linear combination of the terms $a_{n+i}a_{n+j}$ for $0 \leq i \leq j \leq r-1$. As these are $\frac{1}{2}r(r+1)$ many, already an ansatz for a recurrence of this order will lead to an underdetermined linear system.

9. Starting from recurrences for the given sequences, proceed as in the proof of Theorem 2.30 to construct a recurrence of order $r_a + r_b + r_c$ which holds simultaneously for all three sequences. Doing so leads to a linear system with $(r_b + r_c + 1) + (r_a + r_c + 1) + (r_a + r_b + 1) = 2(r_a + r_b + r_c) + 3$ unknowns and $2(r_a + r_b + r_c + 1)$ equations. The corresponding matrix has $r_b + r_c + 1$ columns with entries of degree $\leq d_a$ and $r_a + r_c + 1$ columns of degree $\leq d_b$ and $r_a + r_b + 1$ columns of degree $\leq d_c$. By Theorem 1.29, there is a solution vector whose first $r_b + r_c + 1$ entries have degrees $(r_b + r_c)d_a + (r_a + r_c + 1)d_b + (r_a + r_b + 1)d_c$. This leads to a recurrence with the claimed degree.

10. Define $\tilde{p}_i(x) = p_i(x)q_1(x)\cdots q_1(x+i-1)q_0(x+i+1)\cdots q_0(x+r)$ for $i = 0, \ldots, r$. Then $\tilde{p}_0(n)a_nb_n + \cdots + \tilde{p}_r(n)a_{n+r}b_{n+r} = 0$ for all $n \in \mathbb{N}$.

11. For $c_n = a_n + b_n$ and $d_n = a_nb_n$ we have $(16n^6 + 182n^5 + 819n^4 + 1844n^3 + 2155n^2 + 1212n + 252)c_n + (52n^6 + 600n^5 + 2766n^4 + 6486n^3 + 8115n^2 + 5112n + 1269)c_{n+1} + (112n^6 + 1302n^5 + 6079n^4 + 14528n^3 + 18664n^2 + 12178n + 3157)c_{n+2} + (108n^6 + 1264n^5 + 5962n^4 + 14462n^3 + 18975n^2 + 12740n + 3421)c_{n+3} + (72n^6 + 846n^5 + 4015n^4 + 9816n^3 + 12991n^2 + 8796n + 2380)c_{n+4} = 0$ and $(7168n^8 + 104704n^7 + 646128n^6 + 2195824n^5 + 4482900n^4 + 5607460n^3 + 4171844n^2 + 1673262n + 273735)d_n + (-17920n^8 - 266688n^7 - 1694512n^6 - 5988320n^5 - 12832996n^4 - 17011140n^3 - 13557192n^2 - 5906142n - 1070685)d_{n+1} + (12096n^8 + 188672n^7 + 1251488n^6 + 4600480n^5 + 10221024n^4 + 14000896n^3 + 11491112n^2 + 5135592n + 951060)d_{n+2} + (-80640n^8 - 1230336n^7 - 7987216n^6 - 28790208n^5 - 62942532n^4 - 85312804n^3 - 69841332n^2 - 31484442n - 5969535)d_{n+3} + (145152n^8 + 2229120n^7 + 14637168n^6 + 53526096n^5 + 118806580n^4 + 163157204n^3 + 134596160n^2 + 60548850n + 11290125)d_{n+4} = 0$. We have canceled the common factors because they do not have integer roots.

12. **a.** $(3+2n)b_n + (7+4n)b_{n+1} + (11+5n)b_{n+2} = 0$; **b.** $(128n^3 + 304n^2 + 200n + 33)b_n + (128n^3 + 400n^2 + 412n + 132)b_{n+1} + (800n^3 + 2460n^2 + 2218n + 528)b_{n+2} = 0$; **c.** $2(22n^2 + 51n + 11)b_{n+2} + 2n(11n + 20)b_n + 18b_{n+1} + 32b_{n+3} + (5n + 12)(11n + 9)b_{n+4} = 0$; **d.** $(-2n-3)b_n - 2(n+2)b_{n+1} + (-n-4)b_{n+2} + (5n+11)b_{n+3} = 0$.

13. $(222x^4 + 116x^3 - 101x^2 - 820x)a''(x) + (555x^3 - 815x^2 - 1592x - 164)a'(x) + (111x^2 - 328x + 608)a(x) = 0$.

14. Start from the inhomogeneous differential equation

$$\sum_{i=0}^{r}\sum_{j=0}^{d} p_{r-i,j}x^{j+i}a^{(j)}(x) = Q(x),$$

which appears in the proof of the theorem. This equation has the form $\sum_{j=0}^{d} u_j(x)a^{(j)}(x) = Q(x)$ for certain polynomials $u_j \in C[x]$ of degree at most $j + r$. Application of the operator $QD_x - Q'$ brings this equation into the form

$$\sum_{j=0}^{d}(Q(x)u_j'(x)a^{(j)}(x) + Q(x)u_j(x)a^{(j+1)}(x) - Q'(x)u_j(x)a^{(j)}(x)) = 0$$

which we can also write as

$$\sum_{j=0}^{d+1}(Q(x)u_j'(x) - Q'(x)u_j(x) + Q(x)u_{j-1}(x))a^{(j)}(x) = 0$$

(with the understanding that $u_{d+1} = u_{-1} = 0$). The polynomial coefficients in this equation have the claimed degrees.

15. Start from the inhomogeneous differential equation

$$\sum_{i=0}^{r}\sum_{j=0}^{d} p_{r-i,j}x^{j+i}a^{(j)}(x) = Q(x),$$

which appears in the proof of the theorem, and observe that it can also be made homogeneous by applying the differential operator D_x^r on both sides. This won't affect the degrees of the polynomial coefficients on the left but it will increase the order by r.

16. Addition should lead to recurrences of order $r_a + r_b$ and degree $(r_a + 1)d_b + (r_b + 1)d_a$, as stated in the theorem. Multiplication should lead to recurrences of order $r_a r_b$ and degree $(r_a d_b + r_b d_a)(r_a r_b - r_a - r_b + 2)$. The degree bound stated in the theorem seems to overshoot slightly.

17. **a.** False. If $(a_n)_{n=0}^{\infty}$ is any non-D-finite sequence, then so is $(-a_n)_{n=0}^{\infty}$, and their sum is the zero sequence, which clearly is D-finite. **b.** False. If $(a_n)_{n=0}^{\infty}$ is any non-D-finite sequence, then so are the sequences $a_0, 0, a_1, 0, a_2, 0, \ldots$ and $0, a_0, 0, a_1, 0, \ldots$. Their product is the zero sequence, which clearly is D-finite. **c.** True. Write $(c_n)_{n=0}^{\infty}$ for the interlaced sequence. If this sequence was D-finite, then so were its subsequences $(c_{2n})_{n=0}^{\infty}$ and $(c_{2n+1})_{n=0}^{\infty}$, which by assumption they are not. **d.** False. $(2^n)_{n=0}^{\infty}$ is D-finite but $(2^{n^2})_{n=0}^{\infty}$ is not (cf. Exercise 11 of Sect. 2.1). **e.** True. In fact, this is even true when $(a_n)_{n=0}^{\infty}$ is not D-finite, because the sequence $(a_{n \bmod 5})_{n=0}^{\infty}$ is periodic, and every periodic sequence is D-finite.

18. Asymptotically, we have $F_n \sim \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n$ $(n \to \infty)$, so for any fixed positive integer k, we have $F_{kn} \sim \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{kn}$ $(n \to \infty)$. If $(F_n)_{n=0}^{\infty}$ is the interlacing of k exponential sequences, this would imply $F_{kn} = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{kn}$ for all $n \in \mathbb{N}$. By Binet's formula, we have $F_{kn} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{kn} + (\frac{1-\sqrt{5}}{2})^{kn})$ for all $n \in \mathbb{N}$, which is a contradiction because $(\frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{kn})_{n=0}^{\infty}$ is certainly not the zero sequence.

19. For the second claim, observe that $g(z+1) = \frac{f'(z+1)}{f(z+1)} = \frac{(r(z)f(z))'}{r(z)f(z)} = \frac{r'(z)f(z)+r(z)f'(z)}{r(z)f(z)} = \frac{r'(z)}{r(z)} + g(z)$ and $g(z+2) = \frac{r'(z+1)}{r(z+1)} + g(z+1) = \frac{r'(z+1)}{r(z+1)} + \frac{r'(z)}{r(z)} + g(z)$. We see that $g(z)$, $g(z+1)$, $g(z+2)$ belong to the $\mathbb{C}(z)$-vector space generated by 1 and $g(z)$, so they must be linearly dependent. For the special case $r(z) = z$, the linear dependence corresponds to the recurrence $z\psi(z) - (2z+1)\psi(z+1) + (z+1)\psi(z+2) = 0$.

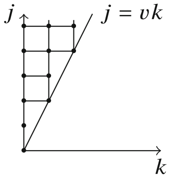
Section 2.4

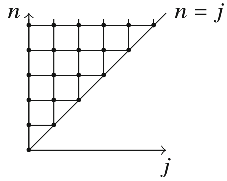
1. According to the binomial theorem, we have $\left(1+\frac{i}{x}\right)^{-n/v} = \sum_{k=0}^{\infty} \binom{-n/v}{k}(i/x)^k$. Therefore,

$$\begin{aligned}
&\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j/v}\sum_{n=0}^{\infty} c_n(x+i)^{-n/v}\\
&=\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j/v}\sum_{n=0}^{\infty} c_n x^{-n/v}\sum_{k=0}^{\infty}\binom{-n/v}{k}(i/x)^k\\
&=\sum_{i=0}^{r}\sum_{j=0}^{\infty}\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} p_{i,j}c_n\binom{-n/v}{k} i^k x^{-(n+j+vk)/v}\\
&=\sum_{k=0}^{\infty}\sum_{j=0}^{\infty}\sum_{n=j+vk}^{\infty}\sum_{i=0}^{r} p_{i,j}c_{n-j-vk}\binom{-(n-j-vk)/v}{k} i^k x^{-n/v}\\
&=\sum_{k=0}^{\infty}\sum_{j=vk}^{\infty}\sum_{n=j}^{\infty}\sum_{i=0}^{r} p_{i,j-vk}c_{n-j}\binom{-(n-j)/v}{k} i^k x^{-n/v}.
\end{aligned}$$

At this point it remains to observe that for any bivariate sequences $a_{k,j}$ and $b_{j,n}$ we have

$$\sum_{k=0}^{\infty}\sum_{j=vk}^{\infty} a_{k,j} = \sum_{j=0}^{\infty}\sum_{k=0}^{\lfloor j/v \rfloor} a_{k,j} \quad \text{and} \quad \sum_{j=0}^{\infty}\sum_{n=j}^{\infty} b_{j,n} = \sum_{n=0}^{\infty}\sum_{j=0}^{n} b_{j,n}.$$





2. For the initial values $f(0) = 0$, $f(1) = 1$, an analogous computation leads to the conjecture $f(n) \sim -\frac{1}{2\pi}(-16)^n n^{-1}$. It follows that for generic initial values α, β, we obtain $f(n) \sim -\frac{2\alpha+\beta}{2\pi}(-16)^n n^{-1}$, unless α, β are such that $2\alpha + \beta = 0$. In that case, the asymptotics is described by the other generalized series solution. For example, for the initial values $f(0) = 1$, $f(1) = -2$, and for

$$h(x) = (-4)^x x^{-1/2}\Big(1 - \tfrac{1}{8}x^{-1} + \tfrac{1}{128}x^{-2} + \tfrac{5}{1024}x^{-3}\Big)$$

and $g(x)$ as in the text, we have

$$\begin{aligned} g(10)/f(10) &\approx 580428 & h(10)/f(10) &\approx 1.7724539926654076731\\ g(100)/f(100) &\approx 2.84467\ 10^{59} & h(100)/f(100) &\approx 1.7724538509171590726\\ g(1000)/f(1000) &\approx 6.43446\ 10^{600} & h(1000)/f(1000) &\approx 1.7724538509055171660. \end{aligned}$$

The values of $h(n)/f(n)$ seem to approach $\sqrt{\pi}$ as $n \to \infty$.

3. The shorter recurrence has the solutions 1 (exact) and $(\frac{1}{2})^n n^{-1/2}(1 - \frac{11}{8}n^{-1} + \frac{457}{128}n^{-2} - \frac{13745}{1024}n^{-3} + \cdots)$. The longer recurrence has the additional solution 2^n (exact). A generic solution of the longer recurrence is a linear combination of 2^n and a generic solution of the first recurrence. If there is a small error in the initial values, the error will grow like 2^n as n increases.

4. The characteristic polynomial of the recurrence is exactly the same as the characteristic polynomial (as defined in linear algebra) of the matrix $\lim_{n\to\infty} P(n)$.

5. **a.** $x^{-1/2}(1 - \frac{7}{16}x^{-1} + \frac{169}{512}x^{-2} - \frac{3085}{8192}x^{-3} + \cdots)$ and $5^x x^{-1/2}(1 - \frac{1}{16}x^{-1} + \frac{25}{512}x^{-2} + \frac{485}{8192}x^{-3} + \cdots)$; **b.** $(-1)^x x^{-1}(1 - \frac{3}{2}x^{-1} + \frac{10}{27}x^{-2} - \frac{10}{81}x^{-3} + \cdots)$ and $8^x x^{-1}(1 - \frac{1}{3}x^{-1} + \frac{1}{27}x^{-2} + \frac{1}{81}x^{-3} + \cdots)$; **c.** $1 + x^{-1} + 2x^{-2} + 8x^{-3} + \cdots$ and $(\frac{1}{2})^x x(1 + x^{-1} + \cdots)$.

6. **a.** $(-1)^x$ and $(-1)^x(\log(x) + \frac{7}{6}x^{-1} - \frac{23}{36}x^{-2} + \frac{35}{81}x^{-3} + \cdots)$; **b.** $\mathrm{e}^{\pm 3x^{1/2}} x^{5/8}(1 - \frac{8}{64}x^{-1} \mp \frac{7}{60}x^{-3/2} + \frac{787}{24576}x^{-2} \pm \frac{977}{80640}x^{-5/2} + \cdots)$; **c.** $\mathrm{e}^{-2x^{1/2}}(x^{-3} + \frac{923}{48}x^{-7/2} +$

$\frac{124325}{576}x^{-4} + \cdots)$ and $e^{-2x^{1/2}}(x^{1/2} + \frac{19}{12} + \frac{131}{240}x^{-1/2} + \frac{7153}{51840}x^{-1} + \frac{183011}{1244160}x^{-3/2} - \frac{142643}{716800}x^{-2} + \frac{58881991451}{18811699200}x^{-5/2} - \frac{24681347272454387}{30958682112000}x^{-7/2} - \frac{328963991034668523198 1}{257452400443392000}x^{-4} + \cdots - (\frac{12775301426933}{2378170368}x^{-4} + \frac{2371124716883}{4954521600}x^{-7/2} + \frac{2568932521}{103219200}x^{-3} + \cdots)\log(x))$

7. Make an ansatz for the recurrence, plug the known solution into it, equate coefficients to zero, solve the resulting linear system. This should give $(x+2)f(x+2) - (10x+15)f(x+1) + (9x+9)f(x) = 0$.

8. Suppose that $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}x^{-j}\log(x+i) = 0$ for some $p_{i,j} \in C$. We show that all $p_{i,j}$ in such a relation must be zero. Using the generalized series of $\log(x+i)$, we have

$$0 = \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}\Big(x^{-j}\log(x) - \sum_{n=1}^{\infty}\frac{(-i)^n}{n}x^{-n}\Big)$$
$$= \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}x^{-j}\log(x) - \sum_{n=1}^{\infty}\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}\frac{(-i)^n}{n}x^{-n-j}.$$

Coefficient comparison yields $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}\frac{(-i)^{n-j}}{n-j} = 0$ for all $n > j$. By the hint, applied with $\phi_i = -i$ $(i = 0,\dots,r)$, it follows that $\sum_{j=0}^{d} p_{i,j}\frac{(-i)^{-j}}{n-j} = 0$ for every i and all $n > j$. If we multiply this equation by $n(n-1)\cdots(n-d)$, it becomes a polynomial relation, and since nonzero polynomials can only have finitely many roots, its validity for all $n > j$ implies its validity for all $n \in \mathbb{Z}$. For any i, we can now set n to any j to obtain $p_{i,j} = 0$, as desired.

This argument only shows that the formal object $\log(x)$ is not D-finite. The non-D-finiteness of the sequence $(\log n)_{n=1}^{\infty}$ is discussed in [196, 210].

9. **a.** If $c \neq 1$, then $(x+1)^\alpha\log(x+1)^m - cx^\alpha\log(x)^m = (1-c)x^\alpha\log(x)^m(1+\cdots)$, and all of these expressions have distinct dominant terms. Therefore, any (finite or infinite) sum of such terms is nonzero, and therefore, there is no f with $f(x+1) - cf(x) = 0$.

Now consider the case $c = 1$. For arbitrary $\alpha \in C$ and $m \in \mathbb{N}$ we have $\Delta x^\alpha\log(x)^m = x^\alpha\log(x)^m(-1 + x^{-m} + (\alpha - \frac{m}{2})x^{-m-1} + \cdots)$, and all of these expressions with $(\alpha, m) \neq (0,0)$ have distinct dominant terms. Again, any (finite or infinite) sum of such terms is nonzero, and therefore, if f is such that $\Delta f = 0$, the only possibility is $f = sx^0\log(x)^0$ for some $s \in C$.

b. The argument is the same as for part a: for every non-constant term

$$\tau = \Gamma(x)^{u/v}\phi^x\exp(P(x^{1/v}))x^\alpha\log(x)^m,$$

the series $\sigma(\tau) - c\tau$ has a different dominant term.

c. We may assume without loss of generality that the series appearing in the linear combination have distinct factorial parts, exponential parts, or subexponential parts, or polynomial parts with irrational degree difference, because any two series in which all of these components agree can be combined into a single one. If the parts are different, then, since shifting only affects the series part, the claim follows from part b.

10. **a.** Let P be a multivariate polynomial P with coefficients in $C[[x^{-1}]][\log(x)]$ which turns zero when the variables are replaced by the quantities in question. We have to show that $P = 0$. If this is not the case, then P must have at least two monomials, otherwise there is no chance for a cancellation.

Let $y_{0,j}$ denote the variables corresponding to x^{α_j}, let $y_{i,j}$ denote the variables corresponding to $\exp(\beta_{i,j}x^{k_i})$ $(i = 1, \dots, n)$, and write z for the variable corresponding to $\Gamma(x)$. Substituting the expressions into a monomial $uz^\ell \prod_{i,j} y_{i,j}^{e_{i,j}}$ gives an expression of the form

$$\Gamma(x)^\ell \exp(\sum_{i,j} e_{i,j}\beta_{i,j}x^{k_i})x^{\operatorname{ord}(u)+\sum_j e_{0,j}\alpha_j}u_0,$$

where $\operatorname{ord}(u)$ refers to the maximal exponent of x appearing in u, and $u_0 = x^{-\operatorname{ord}(u)}u$. Two such expressions are equal iff they share the same ℓ, the same $\operatorname{ord}(u) + \sum_j e_{0,j}\alpha_j$, for each i the same $\sum_j e_{i,j}\beta_{i,j}$, and the same u_0. (This follows from the previous exercise, because the quotient of two such terms would be a constant.) By the assumptions on the linear independence, this means that expressions arising from distinct monomials cannot cancel each other.

b. Write R for the set of all C-linear combinations of generalized series without exponential part. It is clear that R is closed under addition and multiplication, so R is a ring. To see that R is an integral domain, let $f_1, \dots, f_m \in R$ and let $P, Q \in C[y_1, \dots, y_m]$ be such that $P(f_1, \dots, f_m)Q(f_1, \dots, f_m) = 0$. Because of part a, the ring $C[f_1, \dots, f_m]$ is isomorphic to a subring of a multivariate polynomial ring over $C[[x^{-1/v}]][\log(x)]$. Since this ring is an integral domain, it follows that $P = 0$ or $Q = 0$, and since $f_1, \dots, f_m$ were arbitrary, it follows that R is an integral domain.

11. Since S and $\frac{d}{dq}$ are C-linear, it suffices to consider a term $f(x, q) = c(q)x^{q-j/v}\log(x)^k$. We have

$$\begin{aligned}
S\frac{d}{dq} \cdot f(x,q) &= S \cdot (c'(q)x^{q-j/v}\log(x)^k + c(q)x^{q-j/v}\log(x)^{k+1}) \\
&= c'(q)(x+1)^{q-j/v}\log(x+1)^k + c(q)(x+1)^{q-j/v}\log(x+1)^{k+1} \\
\frac{d}{dq}S \cdot f(x,q) &= \frac{d}{dq} \cdot (c(q)(x+1)^{q-j/v}\log(x+1)^k) \\
&= c'(q)(x+1)^{q-j/v}\log(x+1)^k + c(q)(x+1)^{q-j/v}\log(x+1)^{k+1}.
\end{aligned}$$

12. If we have $\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j} f(x+i) = 0$ with $f(x) = \sum_{k=0}^{d}\sum_{n=0}^{\infty} c_{k,n} x^{-n}\log(x)^k$, then $f(x+i) = \sum_{k=0}^{d}\sum_{n=0}^{\infty} c_{k,n}(x+i)^{-n}\bigl(\log(x) - \sum_{\ell=1}^{\infty}\frac{(-i)^\ell}{\ell} x^{-\ell}\bigr)^k$, and hence $[\log(x)^d]f(x+i) = \sum_{n=0}^{\infty} c_{d,n}(x+i)^{-n}$. The key observation is that the last expression is equal to the ith shift of $[\log(x)^d]f(x)$, which is not the case when d is replaced by a smaller exponent.

Since $f(x)$ is a solution of the recurrence, we have $[\log(x)^k]\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j} f(x+i) = 0$ for every $k = 0,\dots,d$. Taking $k = d$ gives $\sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j}[\log(x)^d]f(x+i) = 0$, and because of the key observation, the claim follows.

13. We have

$$
\begin{aligned}
L\cdot x^{-\alpha} &= \sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j}S^i\cdot x^{-\alpha} = \sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j}(\Delta+1)^i\cdot x^{-\alpha}\\
&= \sum_{i=0}^{r}\sum_{j=0}^{\infty} p_{i,j}x^{-j}\sum_{k=0}^{\infty}\binom{i}{k}\Delta^k\cdot x^{-\alpha}\\
&= \sum_{k=0}^{\infty}\sum_{j=0}^{\infty}\sum_{i=0}^{r} p_{i,j}\binom{i}{k}(-\alpha)^{\underline{k}}(x^{-\alpha-j-k}+\cdots)\\
&= \sum_{k=0}^{\infty}\sum_{j=k}^{\infty}\sum_{i=0}^{r} p_{i,j-k}\frac{1}{k!}i^{\underline{k}}(-\alpha)^{\underline{k}}(x^{-\alpha-j}+\cdots)\\
&= \sum_{j=0}^{\infty}\Biggl(\sum_{k=0}^{j}\binom{-\alpha}{k}\sum_{i=0}^{r} p_{i,j-k}i^{\underline{k}}\Biggr)(x^{-\alpha-j}+\cdots).
\end{aligned}
$$

This proves the claimed alternative form for the indicial polynomial.

To see that $\eta = \tilde\eta$, observe first that the expression for η is zero if and only if j is such that $\sum_{i=0}^{r} p_{i,j-k}i^k = 0$ for all $k = 0,\dots,j$. Likewise, the expression for $\tilde\eta$ is zero if and only if j is such that $\sum_{i=0}^{r} p_{i,j-k}i^{\underline{k}} = 0$ for all $k = 0,\dots,j$. Since both $1, x, x^2,\dots$ and $1, x, x^{\underline{2}},\dots$ are bases of the vector space $C[x]$, it follows that $\sum_{i=0}^{r} p_{i,j-k}i^k = 0$ for all $k = 0,\dots,j$ if and only if $\sum_{i=0}^{r} p_{i,j-k}i^{\underline{k}} = 0$ for all $k = 0,\dots,j$. It follows that η and $\tilde\eta$ have the same degree with respect to α.

Next, if j is minimal such that η is nonzero, then we have $\sum_{i=0}^{r} p_{i,j-\ell-k}i^k = 0$ for all $\ell = 0,\dots,j-1$ and all $k = 0,\dots,j$. Therefore, with $S_1(k,\ell)$ denoting the Stirling number of the first kind,

$$
\tilde\eta = \sum_{k=0}^{j}\binom{-\alpha}{k}\sum_{i=0}^{r} p_{i,j-k}i^{\underline{k}} = \sum_{k=0}^{j}\binom{-\alpha}{k}\sum_{i=0}^{r} p_{i,j-k}\sum_{\ell=0}^{k} S_1(k,\ell)i^\ell
$$

$$= \sum_{\ell=0}^{\infty} \sum_{k=0}^{j} \underbrace{S_1(k,\ell)}_{=0 \text{ if } k<\ell} \binom{-\alpha}{k} \underbrace{\sum_{i=0}^{r} p_{i,j-\ell+\ell-k} i^{\ell}}_{=0 \text{ if } k>\ell} = \sum_{k=0}^{j} \binom{-\alpha}{k} \sum_{i=0}^{r} p_{i,j-k} i^k = \eta,$$

as claimed.

14. These are precisely the series of the form $\Gamma(x)^u \phi^x x^\alpha a(x)$ with $u \in \mathbb{Z}$, $\phi, \alpha \in C$ and $a \in C[[x^{-1}]]$.

To see that no other series can arise, observe that the techniques described in this section can produce non-integral exponents of $\Gamma(x)$ or nontrivial subexponential parts or logarithmic terms only for higher order recurrences.

To see that all of these series can arise, observe that if $f(x)$ is any series of the announced form, then we have $\frac{f(x+1)}{x^u f(x)} \in C[[x^{-1}]]$. Therefore, if we denote this quotient by $p(x)$, we have the recurrence $f(x+1) - x^u p(x) f(x) = 0$.

15. $\Gamma(x)\phi^x x^{\alpha+1}(\phi^{-1} + \frac{1+\phi-\alpha\phi}{\phi^2}x^{-1} - \frac{-\alpha^2\phi^2+3\alpha\phi^2+4\alpha\phi-2\phi^2-6\phi-2}{2\phi^3}x^{-2} + \cdots)$

16. Any rational function can be expanded as a Laurent series in descending powers of x, i.e., as element of $C((x^{-1})) = \bigcup_{\alpha\in\mathbb{Z}} x^\alpha C[[x^{-1}]]$. The indicial polynomial of the proposed equation is $1 - 2x$, which has no solutions in $\mathbb{Z}$. Therefore, there is no generalized series solution in $C((x^{-1}))$ and therefore in particular no solution in $C(x)$.

17. Let $d = \max_{i=0}^{r} \deg(p_i)$ and write $p_i = \sum_{j=0}^{d} p_{i,j}(x+i)^{\underline{j}}$, as in the proof of Theorem 2.33. Note that $[x^d]p_i = p_{i,d}$ for all d, so $\chi = \sum_{i=0}^{r} p_{i,d}x^i$. The proof of Theorem 2.33 leads to an inhomogeneous differential equation $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{r-i,j}x^{j+i}a^{(j)}(x) = Q(x)$ for a certain polynomial Q. The polynomial coefficient of the highest order derivative $a^{(d)}(x)$ is $\sum_{i=0}^{r} p_{r-i,d}x^{d+i} = x^d \sum_{i=0}^{r} p_{i,d}x^{r-i} = x^{r+d}\chi(1/x)$. The application of $QD_x - Q'$ to the differential equation leads to a homogeneous equation in which the polynomial coefficient of $a^{(d+1)}(x)$ is $Qx^{r+d}\chi(1/x)$.

18. The subexponential part originates from an edge of slope $1-1/p = (p-1)/p$ in the Newton polygon. Because of $v = 1$, the coordinates of the vertices of the Newton polygon are integers. Therefore, an edge with the desired slope must have a width of kp for some positive integer k. This implies the lower bound on the order. For the same reason, the horizontal distance between any two internal vertices of that edge must be an integer multiple of p. This implies that we have $\mu = s^i u(s^p)$ for some polynomial $u \in C[s]$. It follows that whenever σ is a nonzero root of μ, then so is $\omega\sigma$.

19. **a.** Terms like $\mathrm{e}^{x^{-2}}$ can be incorporated into the series part by $\mathrm{e}^{-x^2} = \sum_{n=0}^{\infty} \frac{1}{n!}x^{-2n}$. **b.** A substitution $f(x) = \mathrm{e}^{x^c}g(x)$ would introduce terms $\mathrm{e}^{(x+i)^c}/\mathrm{e}^{x^c} = \mathrm{e}^{x^c(1-i/x)^c - x^c} = \mathrm{e}^{-cix^{c-1}+\mathrm{O}(x^{c-2})}$ into the coefficients of the recurrence, and such terms cannot be identified with elements of $C[[x^{-1/v}]]$ for any $v \in \mathbb{N}$.

20. Writing $f(x)$ for the unknown series, the determinant

$$\begin{vmatrix} f(x) & f_1(x) & \cdots & f_r(x) \\ f(x+1) & f_1(x+1) & \cdots & f_r(x+1) \\ \vdots & \vdots & \ddots & \vdots \\ f(x+r) & f_r(x+r) & \cdots & f_r(x+r) \end{vmatrix}$$

is a linear combination of $f(x), \ldots, f(x+r)$ whose coefficients are generalized series. (Observe that the product of two generalized series is a generalized series.) Since the series $f_i(x)$ do not contain logarithmic terms, all quotients $f_i(x+j)/f_i(x)$ are series in $C[[x^{-1/v}]]$ for a suitable $v \in \mathbb{N}$. Therefore, dividing the determinant by the product $f_1(x) \cdots f_r(x)$ leads to a recurrence of the desired form. The linear independence of $f_1(x), \ldots, f_r(x)$ guarantees that the recurrence is not identically zero. On the other hand, the determinant obviously becomes zero when $f(x)$ is replaced by any $f_i(x)$. Therefore all of these series are solutions of the recurrence, as desired.

Section 2.5

1. $\sum_{k=0}^{n}(-1)^{n+k}\binom{n}{k}\sum_{i=0}^{n} a_i\binom{k}{i} = \sum_{i=0}^{n} a_i \sum_{k=0}^{n}(-1)^{n+k}\binom{k}{i}\binom{n}{k}$. To complete the proof, it suffices to show that $\sum_{k=0}^{n}(-1)^{n+k}\binom{k}{i}\binom{n}{k} = \delta_{i,n}$. Reversing the order of summation, using $\binom{n}{n-k} = \binom{n}{k}$, the identity from the hint, and the summation formula $\sum_{k=0}^{n}(-1)^{k}\binom{x}{k} = (-1)^{n}\binom{x-1}{n}$, we get $\sum_{k=0}^{n}(-1)^{n+k}\binom{k}{i}\binom{n}{k} = \sum_{k=0}^{n}(-1)^{2n-k}\binom{n}{i}\binom{n-i}{k} = \binom{n}{i}\sum_{k=0}^{n}(-1)^{k}\binom{n-i}{k} = (-1)^{n}\binom{n}{i}\binom{n-i-1}{n} = \delta_{i,n}$, as required.

2. We have $[S_n^0]S_n^d M = \sum_{i=0}^{r} p_{i,d}[S_n^{-d}]((n+d)S_n^{-1})^d$, because all other terms contributing to M have higher degree in S_n. Using the commutation rule $S_n^{-1}p(n) = p(n-1)S_n^{-1}$ for polynomials p, we have $(n+d)S_n^{-1}(n+d)S_n^{-1}\cdots(n+d)S_n^{-1} = (n+d)(n+d-1)\cdots(n+1)S^{-d}$. The trailing coefficient is therefore $(n+d)^{\underline{d}}\sum_{i=0}^{r} p_{i,d}$.

3. $f(x) = p(x)$ is a solution of the recurrence $p(x+1)f(x) - p(x)f(x+1) = 0$.

4. A necessary condition for the existence of polynomial solutions is that the characteristic polynomial has 1 among its roots. Since $2-2+3+8 = 11 \neq 0$, this is not the case for the given recurrence.

5. The solution spaces in $\mathbb{Q}[x]$ are generated by **a.** $1, x$; **b.** $100648 + 23490x + 2003x^2 + 74x^3 + x^4$; **c.** $(x-1)(x-2)(x-3)(x-4)$; **d.** $\emptyset$.

6. The solution spaces in $\mathbb{Q}[x] \times \mathbb{Q}^m$ are generated by **a.** $(26x+5, -60, -70)$; **b.** $(8+16x+x^2, 1, 0)$, $(7x^2+x^2, 0, 1)$; **c.** $\emptyset$; **d.** $((x-1)(x-2)(x-3)(x-4), 0)$, $(110x+101x^2+70x^3+7x^4, 288)$.

7. Regardless of the choice of α, the indicial polynomial is $x - 3$, so any polynomial solution must have the form $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ for some $a_0, \dots, a_3 \in C$. Plug the ansatz into the recurrence and equate coefficients of x^i to zero. This gives a linear system of size 5×4 whose entries still contain the unknown parameter α. Using Gaussian elimination, it can be shown that this system has a nontrivial solution if and only if $\alpha = 23$.

8. Plug an ansatz $f(x) = a_0 + a_1x + a_2x^2$ with unknown coefficients a_0, a_1, a_2 into the equation and equate coefficients. This leads to a linear system over C with five variables a_0, a_1, a_2, c_1, c_2 and four equations (the coefficients of x^0, x^1, x^2, x^3). As the system has more variables than equations, it must have a nontrivial solution.

9. We may replace K by the smallest subfield of K which contains all the coefficients of the given equation. Then K is finitely generated as $C(x)$-vector space. Let $b_1, \dots, b_d \in K$ be a basis. Write the recurrence in the form $\sum_{i=0}^{r} \sum_{j=1}^{d} p_{i,j} b_j f(x+i) = 0$ with $p_{i,j} \in C(x)$. It then suffices to determine the solution spaces of the recurrences $\sum_{i=0}^{r} p_{i,j} f(x+i) = 0$ for all $j = 1, \dots, d$. Their intersection is the solution space of the original recurrence.

10. We may replace K by the smallest subfield of K which contains all the right hand sides. Then K is finitely generated as $C(x)$-vector space. Choose a basis $b_1, \dots, b_d \in K$ with $b_1 = 1$. Then we can write the equation in the form $\sum_{i=0}^{r} p_i(x) f(x+i) = \sum_{i=1}^{m} c_i g_i$ for some $g_i \in K$ which we may write as $g_i = \sum_{j=1}^{d} q_{i,j} b_i$ for some $q_{i,j} \in C(x)$.

For every choice $f \in C(x)$, the left hand side will evaluate to an element of $C(x)$. We can therefore equate coefficients of b_i and obtain one parameterized recurrence equation $\sum_{i=0}^{r} p_i(x) f(x+i) = \sum_{i=1}^{m} c_i q_{i,1}$ and $d-1$ linear constraints $\sum_{i=1}^{m} c_i q_{i,j} = 0$ for $j = 2, \dots, d$. We can determine the solution space of the recurrence and the solution space for the system of linear constraints and determine their intersection.

11. For every root ϕ of the characteristic equation, apply a substitution $f(x) = \phi^x \tilde{f}(x)$. After dividing the resulting equation for $\tilde{f}(x)$ by ϕ^x, it has polynomial coefficients. Then use one of the algorithms discussed in the text to find its polynomial solutions $\tilde{f}(x)$.

12. The solution space of the recurrence is generated by the sequences b_1, b_2 with $b_1(n) = (n-3)(n-4)(n-5)(n-6)$ and $b_2(n) = (n-1)(n-2)(n-3)(n-4)$. The sequence a must be a linear combination $a_n = \alpha_1 b_1(n) + \alpha_2 b_2(n)$. Comparison with the initial values gives the linear system $5 = 360\alpha_1 + 24\alpha_2$, $2 = 120\alpha_1$ which has the unique solution $(\alpha_1, \alpha_2) = (1/60, -1/24)$. Therefore $a_n = \frac{1}{120}(-3n^4 + 14n^3 + 63n^2 - 434n + 600)$.

13. It suffices to show that the recurrence $q(x+1) - q(x) = p(x+1)$ has a polynomial solution. From Lemma 2.55 we get the degree bound $\deg(q) \leq \deg(p) + 1 =: n$. Consider the ansatz $q(x) = q_0 + q_1x + \cdots + q_nx^n$ and the parameterized recurrence $q(x+1) - q(x) = cp(x+1)$ for unknown c. Plug the ansatz into the equation and equate coefficients. Because of $\deg(q(x+1) - q(x)) < n$, this leads to a linear system over C with $n+2$ variables ($n+1$ from q and 1 from the right hand side) and n equations. Thus there are at least two linearly independent solutions. As the solution space of the homogeneous equation $q(x+1)-q(x)=0$ has dimension 1 (it is generated by the constant solution 1), there must be some solution (q,c) with $c\neq 0$. Then also $(\frac{1}{c}q,1)$ is a solution, so we have $\sum_{k=0}^{n} p(k) = \frac{1}{c}q(n)$ for all n.

14. False. Counterexample: $f(x)=x^3+1$ satisfies $2(1+x)(2+x)(3+x)f(x) - 2(1+x)(3+x)(1+2x)f(x+1)+2x(1+x)(2+x)f(x+2)=0$.

15. For example, the solution space of the operator $(S-1)^k(S-2)^{r-k}$ is generated by x^i for $i=0,\dots,k-1$.

16. Suppose $p(x+i)$ is not irreducible for some $i\in\mathbb{Z}$, say $p(x+i)=v(x)u(x)$ for some $u,v\in C[x]\setminus C$. Then $p(x)=v(x-i)u(x-i)$, and this factorization is nontrivial because $\deg v(x-i)=\deg v(x)$ and $\deg u(x-i)=\deg u(x)$.

17. Suppose $i,j\in\mathbb{Z}$ are such that there exists a $k\in\mathbb{Z}$ for which $g(x)=\gcd(p(x+i),q(x+k+j))$ is nontrivial. Then $\gcd(p(x),q(x+k+j-i))=g(x-i)$ is nontrivial, so p and q are not shift-coprime.

18. $\{0,2,3,5,6\}$

19. "$\subseteq$": If $i\in\operatorname{Spread}(a,bc)$ then $\gcd(a(x),b(x+i)c(x+i))\neq 1$. Let $q(x)$ be an irreducible factor. Then $q(x)\mid a(x)$ and $q(x)\mid b(x+i)c(x+i)$. Then $q(x)\mid b(x+i)$ or $q(x)\mid c(x+i)$, so $q(x)\mid\gcd(a(x),b(x+i))$ or $q(x)\mid\gcd(a(x),c(x+i))$, so $i\in\operatorname{Spread}(a,b)\cup\operatorname{Spread}(a,c)$.

"$\supseteq$": If $i\in\operatorname{Spread}(a,b)\cup\operatorname{Spread}(a,c)$ then $i\in\operatorname{Spread}(a,b)$ or $i\in\operatorname{Spread}(a,c)$. If $i\in\operatorname{Spread}(a,b)$ then $\gcd(a(x),b(x+i))$ is nontrivial. Then in particular $\gcd(a(x),b(x+i)c(x+i))$ is nontrivial, so $i\in\operatorname{Spread}(a,bc)$. The case $i\in\operatorname{Spread}(a,c)$ is analogous.

20. This follows from $\gcd(a(x),b(x+i))\neq 1 \iff \gcd(a(x+k),b(x+k+i))\neq 1$.

21. Rewrite the recurrence equation in the form

$$f(x+r)=\frac{1}{p_r(x)}\Big(g(x)-\sum_{i=0}^{r-1}p_i(x)f(x+i)\Big).$$

By repeatedly using the recurrence, every $f(x+r+i)$ with $i\geq 0$ can be written as a $C(x)$-linear combination of $f(x),\dots,f(x+r-1)$. More specifically, there are polynomials $a_0,\dots,a_{r-1}\in C[x]$ such that

$$f(x+r+s)=\frac{g(x)-\sum_{i=0}^{r-1}a_i(x)f(x+i)}{p_r(x)p_r(x+1)\cdots p_r(x+s)}$$

The denominator of the rational function on the left is $v(x+r+s)$ while the denominator on the right is (a divisor of) $p_r(x)p_r(x+1)\cdots p_r(x+s)v(x)\cdots v(x+$

$r-1$). By Theorem 2.62 and the choice of s, we have $\gcd(v(x+r+s), v(x+i)) = 1$ for $i = 0, \dots, r-1$. Therefore $v(x+r+s) \mid \prod_{i=0}^{s} p_r(x+i)$ and therefore $v(x) \mid \prod_{i=0}^{s} p_r(x+i-(r+s)) = \prod_{i=0}^{s} p_r(x-r+i)$, as claimed.

22. Suppose otherwise. Then $\gcd(v(x-i), \prod_{k=0}^{n} u(x+k)) \neq 1$ or $\gcd(\prod_{k=0}^{n} v(x-k), u(x+i)) \neq 1$ for some $i \in \{s+1, \dots, n\}$. In the first case, we have $\gcd(v(x-i), u(x+k)) \neq 1$ for some $i \in \{s+1, \dots, n\}$ and some $k \in \{0, \dots, n\}$, so $\gcd(v(x), u(x+i+k)) \neq 1$, so $\operatorname{Disp}(v, u) \geq i+k > s$, a contradiction. The second case is excluded analogously.

23. The respective solution spaces in $\mathbb{Q}(x)$ are generated by **a.** $\frac{1}{(2x-3)(2x-5)(x-1)(x-2)(x-3)(x-4)(x-5)}$ and $\frac{1}{(x-3)(x-4)(x-5)}$; **b.** $\emptyset$; **c.** $(2x-1)(2x-3)$, $\frac{1}{(2x-3)(2x-5)}$; **d.** $\frac{(x-5)(3x-1)}{(x-4)(x-3)(x-2)(3x+1)(3x+4)(3x+7)(3x+10)}$.

24. Bases of the solution spaces are **a.** $\{(\frac{2x+5}{(x+1)(x+2)(x+3)}, 0, 0, 0)$, $(\frac{10x^3+44x^2-127}{(x+1)(x+2)(x+3)}, 80, -96, 32)\}$; **b.** $\{(\frac{x}{(x+1)(x+2)}, -6, 0), (1, -34, -6)\}$.

25. If H_n was rational, then the recurrence $f(x+1) - f(x) = 1/(x+1)$ would have a rational solution. This is not the case.

26. The expansion of $1/v$ as a generalized series has the form $cx^{-k} + \cdots$ where $c \neq 0$ and where $k \in \mathbb{N}$ is the multiplicity of x in v. Therefore, every generalized series solution $f(x) = x^{\alpha} + \cdots$ of the original equation corresponds to a generalized series solution $\tilde{f}(x) = cx^{\alpha-k} + \cdots$ of the new equation. Therefore, $\eta(x) = \tilde{\eta}(x+k)$.

27. False. It might be that one equation has a rational solution while the other does not. Then for one of them the denominator bound must be nontrivial while for the other we can take $v = 1$. For example, $xf(x+1) - xf(x) = 1$ has no solution while $xf(x+1) - xf(x) = x$ does.

28. We found the following values:

	0	1	2	3	4	5	6	7	8	9	10
a.	0	0	0	−1	−2	−2	−1	−1	−1	−1	−1
b.	0	0	0	0	−1	−1	−1	0	0	0	0
c.	0	0	0	0	−1	−1	−1	0	0	0	0.

29. Abramov's denominator bound corresponds to the worst case of van Hoeij's denominator bound, in the following sense. Define $\nu_1 \colon \mathbb{Z} \to \mathbb{Z}$ recursively by $\nu_1(n) = 0$ for $n < 0$ and $\nu_1(n) = \nu_1(n-1) + m$, where m is the multiplicity of $(x-r-\alpha-n)$ in the leading coefficient p_r of the recurrence. Furthermore, define $\nu_2 \colon \mathbb{Z} \to \mathbb{Z}$ recursively by $\nu_2(n) = 0$ for $n > s$ and $\nu_2(n) = \nu_2(n+1) + m$, where m is the multiplicity of $(x-\alpha-n)$ in the trailing coefficient p_0 of the recurrence. Then the function $\nu \colon \mathbb{Z} \to \mathbb{Z}$, $\nu(n) = \min(\nu_1(n), \nu_2(n))$ gives Abramov's denominator bound.

30. Consider a first order equation $v(x)f(x) - u(x)f(x+1) = 1$ and suppose that $f(x)$ is a polynomial solution. If $p(x)$ is an irreducible factor of $f(x)$, then $p(x) \mid$

$v(x)f(x)$ implies $p(x) \mid u(x)f(x+1)$, so $p(x) \mid u(x)$ or $p(x) \mid f(x+1)$. Similarly, if $p(x) \mid f(x+1)$ then $p(x-1) \mid f(x)$ implies $p(x-1) \mid u(x)$ or $p(x-1) \mid f(x+1)$. Repeating the argument, we must eventually reach a nonnegative integer $i \in \mathbb{N}$ such that $p(x-i) \nmid f(x+1)$ and $p(x-i) \mid u(x)$. In the other direction, if $p(x)$ is an irreducible factor of $f(x)$, then $p(x+1)$ is an irreducible factor of $f(x+1)$, so $p(x+1) \mid v(x)f(x)$, so $p(x+1) \mid v(x)$ or $p(x+1) \mid f(x)$. Repeating the argument, we must eventually reach a nonnegative integer $j \in \mathbb{N}$ such that $p(x+1+j) \nmid f(x)$ and $p(x+1+j) \mid v(x)$. Then $\gcd(u(x-1), v(x-(i+j))) = p(x-i) \neq 1$, as required.

31. $\{3\}$ and $\mathbb{Z}$. Note that x is the only monic irreducible polynomial which can cause the spread to be infinite with respect to σ.

Section 2.6

1. If P is such that $P(x, y) = 0$, then $P(x, r\bar{y}) = 0$, and if P is such that $P(x, \bar{y}) = 0$, then $P(x, y/r) = 0$.

2. By the previous exercise, it suffices to show that the only algebraic kernels are constant multiples of ω^x. Let y be a kernel, $\sigma(y)/y = u/v$ with coprime $u, v \in C[x]$, and suppose that $P(x, y) = 0$ for some $P \in C(x)[z] \setminus \{0\}$. We may assume that $P = p_0 + p_1 z + \cdots + p_d z^d$ is chosen of minimal possible degree d with respect to z, and that $p_d = 1$. Since P cannot just be a monomial, there must be some $i < d$ with $p_i \neq 0$. Fix such an i. Since d is minimal and $P(x+1, \frac{u}{v}y) - (\frac{u}{v})^d P(x, y) = 0$ is a polynomial equation of degree less than d, it must be identically zero, so we have $\sigma(p_i)(\frac{u}{v})^i = (\frac{u}{v})^d p_i$. Since y is a kernel, $\sigma(p_i)/p_i = (\frac{u}{v})^{d-i}$ forces p_i to be a constant, because if w were an irreducible factor of p_i, then $\sigma(w)$ would be an irreducible factor of $\sigma(p_i)$, so $\sigma(w) \mid \gcd(u, \sigma(v))$. Now that we know that p_i is a constant, we have $\sigma(p_i)/p_i = 1 = (\frac{u}{v})^{d-i}$, so $\frac{u}{v}$ is a root of unity, as claimed.

3. Let $u_1, u_2 \in C(x)$ be such that $\sigma(y_1)/y_1 = u_1$, $\sigma(y_2)/y_2 = u_2$.

"$\Rightarrow$": If $\sigma(y_1 + y_2)/(y_1 + y_2) = r \in C(x)$, then $u_1 y_1 + u_2 y_2 = r y_1 + r y_2$, so $(u_1 - r)y_1 = (r - u_2)y_2$. If $u_1 \neq r$ or $u_2 \neq r$, it follows that y_1 and y_2 are similar. If $u_1 = r$ or $u_2 = r$, then $u_1 = u_2 = r$, because $y_1, y_2 \neq 0$, and then y_1/y_2 is a constant, because $\sigma(y_1/y_2) = (u_1 y_1)/(u_2 y_2) = y_1/y_2$. So by assumption on the constant field, it follows again that $y_1/y_2 \in C(x)$ and y_1, y_2 are similar.

"$\Leftarrow$": If y_1, y_2 are similar, say $y_1/y_2 = r \in C(x)$, then $r \neq -1$ by the assumption $y_1 + y_2 \neq 0$, and therefore $\sigma(y_1 + y_2)/(y_1 + y_2) = \sigma((1+r)y_2)/((1+r)y_2) = u_2 \sigma(1+r)/(1+r) \in C(x)$.

4. The sequence satisfies a recurrence of the form $p(n)a(n) - q(n)a(n+1) = 0$ for some nonzero polynomials $p, q \in C[x]$. The polynomial q has only finitely many roots, so there exists $n_0 \in \mathbb{Z}$ such that $q(n) \neq 0$ for all $n \geq n_0$. Therefore, if $a(n_0) = 0$ then $a(n) = 0$ for all $n \geq n_0$ and if $a(n_0) \neq 0$ then $a(n) \neq 0$ for all $n \geq n_0$.

5. $a(n) = \frac{1}{2}\binom{2n}{n} + \frac{3}{2}2^n - n.$

6.

Input: A hypergeometric term y.
Output: $r \in C(x)$ such that y/r is a kernel.

Set $r = 1$, and let $u, v \in C[x]$ be such that $\sigma(y)/y = u/v$.
while there exists $i \in \mathbb{Z}$ such that $\gcd(u, \sigma^i(v)) \neq 0$, do
  Choose such an i and let $q = \gcd(u, \sigma^i(v))$.
  if $i < 0$ then
    $r = r/(q \cdots \sigma^{-i+1}(q))$
  else
    $r = \sigma^{-i}(q) \cdots \sigma^{-1}(q)\, r$
  $u = u/q,\ v = v/\sigma^{-i}(q)$
Return r.

7. Let y be such that $\sigma(y)/y = u/v$. If $\gcd(u, \sigma^i(v)) = 1$ for all positive integers i, then we can take $a = 1$, $b = u$, $c = \sigma^{-1}(v)$, and we are done. Otherwise, let $i \in \mathbb{N}$ be maximal such that $p := \gcd(u, \sigma^i(v)) \neq 1$. With $a = p\sigma(p)\cdots\sigma^{i-1}(p)$ we have $\frac{u}{v} = \frac{\sigma a \bar{u}}{a \bar{v}}$ for some $\bar{u}, \bar{v} \in C[x]$ with $\gcd(\bar{u}, \sigma^j(\bar{v})) \neq 1$ for all $j \geq i$.

By repeating this construction, if necessary, we eventually arrive at polynomials $a, b, c \in C[x]$ with $\frac{u}{v} = \frac{\sigma(a)}{a}\frac{b}{c}$ and $\gcd(b, \sigma^i(c)) = 1$ for all $i \in \mathbb{N}$. Replacing c by $\sigma^{-1}(c)$ gives a decomposition which satisfies the requirements (i) and (ii).

If the third condition is violated, say $g = \gcd(a, b) \neq 1$, we can replace a by $a' = a/g$ and b by $b' = \sigma(g)b/g$. We then have $\frac{u}{v} = \frac{\sigma(a')}{a'}\frac{b'}{\sigma(c)}$ and $\gcd(b', \sigma^i(c)) = 1$ for all positive integers i. (If we had $\gcd(b', \sigma^i(c)) \neq 1$ for some positive integer i, we would have $\gcd(b, \sigma^{i+1}(c)) \neq 1$ by the choice of b', and this is not the case.) Repeating this construction, if necessary, we eventually arrive at a decomposition which also satisfies $\gcd(a, b) = 1$ (note that $\deg(a)$ is getting smaller in each iteration).

The requirement $\gcd(a, c) = 1$ can be achieved in the same way.

8. Suppose that y is a hypergeometric solution with $\sigma(y)/y = r \in C(x)$, and consider the representation $r(x) = \phi\frac{a(x+1)}{a(x)}\frac{b(x)}{c(x+1)}$ of Exercise 7. Plug y into the input recurrence, divide by y, and clear denominators. This gives

$$\bar{p}_0(x)a(x) + \bar{p}_1(x)\phi a(x+1) + \cdots + \bar{p}_r(x)\phi^r a(x+r) = 0,$$

where the $\bar{p}_i(x) \in C(x)$ are defined as in line 4 of the algorithm but with b in place of u and $\sigma(c)$ in place of v.

Since $b \mid \bar{p}_i$ for $i = 1, \ldots, r$, we must have $b \mid \bar{p}_0 a$, which by the choice of a, b, c requires $b \mid p_0$. Likewise, since $\sigma^r(c) \mid \bar{p}_i$ for $i = 0, \ldots, r-1$, we must have $c \mid \sigma^{-r}(\bar{p}_r)a$, which by the choice of a, b, c requires $c \mid \sigma^{-r}(p_r)$.

Hence, as the algorithm iterates over all pairs (u, v) of monic divisors of p_0 and $\sigma^{-r}(p_r)$, it will in one iteration consider the choice $(u, v) = (b, \sigma(c))$, and in this iteration, it finds $a \in C[x]$ as polynomial solution of the equation in line 6.

9. For simplicity, assume that $k > 0$. The case $k < 0$ is analogous, the case $k = 0$ is trivial. Set $w = u' \cdots \sigma^{k-1}(u')$. Then for $i = 0, \dots, r$ we get

$$\begin{aligned}\bar{p}_i &= p_i u \cdots \sigma^{i-1}(u)\sigma^i(v) \cdots \sigma^{r-1}(v) = p_i \sigma^k(u') \cdots \sigma^{k+i-1}(u') \\ &= p_i u' \cdots \sigma^{i-1}(u')\sigma^i(v) \cdots \sigma^{r-1}(v)\frac{\sigma^i(w)}{w} = \bar{p}_i' \frac{\sigma^i(w)}{w},\end{aligned}$$

where $\bar{p}_i'$ refers to the value of $\bar{p}_i$ in the iteration corresponding to u'. Therefore, $q \in C(x)$ is a solution of the recurrence of line 6 for the iteration corresponding to u if and only if $wq \in C(x)$ is a solution of this recurrence in the iteration corresponding to u'.

In the iteration for u, a rational solution q gives rise to a hypergeometric solution y with $\frac{\sigma(y)}{y} = \phi\frac{\sigma(q)u}{qv}$. In the iteration for u', the rational solution wq gives rise to a hypergeometric solution y' with $\frac{\sigma(y')}{y'} = \phi\frac{\sigma(qw)u'}{qwv} = \phi\frac{\sigma(q)\sigma^k(u')}{qv} = \frac{\sigma(q)u}{qv} = \frac{\sigma(y)}{y}$. Therefore, every solution found in the iteration for u corresponds to a solution found in the iteration for u'. An analogous argument confirms the other inclusion.

10. **a.** $(2x+1)!/x!^2$ and $(-1)^x$; **b.** $x\binom{2x}{x}$; **c.** no hypergeometric solutions; **d.** $\alpha(2x+3)2^x + \beta(5x+3)(5x+8)(5x+11)2^x$ for arbitrary $\alpha, \beta \in C$

11. **a.** Suppose that they are linearly dependent, and assume without loss of generality that every proper subset of $\{y_1, \dots, y_n\}$ is linearly independent (if this is not the case, discard some of the terms). Then every linear dependence $a_1y_1 + \cdots + a_ny_n = 0$ with $a_1, \dots, a_n \in C(x)$ is such that $a_i \neq 0$ for all i. Let $u_1, \dots, u_n \in C(x)$ be such that $\sigma(y_i)/y_i = u_i$ for $i = 1, \dots, n$. Then $\sigma(a_1y_1 + \cdots + a_ny_n) = \sigma(a_1)u_1y_1 + \cdots + \sigma(a_n)u_ny_n = 0$ and $(\sigma(a_n)u_na_1 - a_n\sigma(a_1)u_1)y_1 + \cdots + (\sigma(a_n)u_na_{n-1} - a_n\sigma(a_{n-1})u_{n-1})y_{n-1} = 0$. Since $y_1, \dots, y_{n-1}$ are linearly independent, this implies $\sigma(a_n)u_na_i - a_n\sigma(a_i)u_i = 0$ for all i. Writing this in the form $u_n = \frac{\sigma(a_i/a_n)}{a_i/a_n}u_i$, we see that y_n and y_i are similar. **b.** This follows directly from part a, for if $y = a_1y_1 + \cdots + a_ny_n$ for certain $a_1, \dots, a_n \in C(x)$, then $p_0y + \cdots + p_r\sigma^r(y) = a_1q_1y_1 + \cdots + a_nq_ny_n$ for certain rational functions $q_1, \dots, q_n$, so if one of the a_i is nonzero, the corresponding q_i must be zero, and then it follows that already y_i is a solution of the recurrence.

12. If y is any hypergeometric term, then $p_0y + \cdots + p_r\sigma^r(y)$ is either zero or similar to y. Therefore, in order for a hypergeometric term y to be a solution of the inhomogeneous recurrence, it must be similar to h. We can therefore make an ansatz $y = qh$ for some unknown rational function, plug this ansatz into the equation and divide on both sides by h. Writing $u = \sigma(h)/h$, the new equation has the form $p_0q + p_1u\sigma(q) + \cdots + p_ru\sigma(u)\cdots\sigma^{r-1}(u)\sigma^r(q) = 1$. Every hypergeometric solution y of the original equation corresponds to a rational solution q of this new equation, so we can solve the problem using the techniques of the previous section.

By the previous exercise, in order to solve the summation problem, it suffices to check that the recurrence $\sigma(y) - y = \binom{2(x+1)}{x+1}$ has no hypergeometric solution.

13. $\alpha = -1$ and $\alpha = 1$.

14. False. For a counterexample, it suffices to show that the sum of two solutions with nonnegative valuation growth may have negative valuation growth. For example, for two sequences f_1, f_2 with $\liminf_{n\to-\infty} \nu(f_1(n)) = 0$ and $\liminf_{n\to-\infty} \nu(f_2(n)) = 1$, we certainly have $\liminf_{n\to-\infty} \nu(f_1(n) + f_2(n)) = 0$. If we also have $\liminf_{n\to\infty} \nu(f_1(n)) = \liminf_{n\to\infty} \nu(f_1(n)) = \liminf_{n\to\infty} \nu(f_1(n) + f_2(n)) = 0$, then the valuation growth of f_1 and $f_1 + f_2$ is zero, but that of $f_2 = (f_1 + f_2) - f_1$ is negative.

For a concrete example of this kind, consider the recurrence $(x + 1)f(x) - (x^2 + 3x + 1)f(x + 1) + x(x + 2)f(x + 2) = 0$ with its two linearly independent hypergeometric solutions $f_1 = 1$ and $f_2 = 1/x!$. The corresponding solutions in $C((q))^{\mathbb{Z}}$ of the deformed recurrence have the requirements stated above.

15. Suppose otherwise. Then $\sigma(y)/y = u/v$ is a rational function in which at least one of the polynomials u, v has positive degree. Let us consider the case $\deg(u) > 0$, the case $\deg(v) > 0$ is similar. If $\deg(u) > 0$, then u has a root $\alpha \in C$. Since y is a kernel, $\alpha + i$ is not a root of v for any $i \in \mathbb{Z}$. Consider the sequence $f : \alpha + \mathbb{Z} \to C((q))$ defined by $f(\alpha) = 1$ and $v(n+q)f(n+1) - u(n+q)f(n)$ for all $n \in \alpha + \mathbb{Z}$. Since α is a root of u, say of multiplicity $\nu > 0$, but not a root of v, the series $f(\alpha)$ has order $\nu > 0$. Since $v(n + \alpha) \neq 0$ for all $n \in \mathbb{Z}$, it follows that $f(\alpha + n)$ has order at least ν for all $n > 0$. Hence the valuation growth of y at the class $\alpha + \mathbb{Z}$ is at least ν, and thus positive. This is in conflict with the assumption.

16. **a.** 1 and $\sum_{k=1}^n \frac{1}{k^2}$; **b.** $\binom{2n}{n}$ and $\binom{2n}{n}\sum_{k=0}^n 1/\binom{2k}{k}$; **c.** $\frac{1}{n!}$, $\frac{1}{n!}\sum_{k=0}^n k!$, and $\frac{1}{n!}\sum_{k=0}^n k! \sum_{i=0}^k \binom{2i}{i}$; **d.** 1, $\sum_{k=1}^n \frac{1}{k}$, and $\sum_{k=1}^n \frac{1}{k}\sum_{i=2}^k \frac{2i-1}{i(i-1)}$.

17. By definition of the a_i, we have $(v_{i-1}S - u_{i-1}) \cdot a_i = a_{i-1}$ for all $i > 0$. This implies the claim in the hint. It is also clear from the definition of the a_i that $(v_{i-1}S - u_{i-1}) \cdots (v_1 S - u_1) \cdot a_j = 0$ for all $j < i$. Therefore, applying $(v_{i-1}S - u_{i-1}) \cdots (v_1 S - u_1)$ to any linear combination $\alpha_1 a_1 + \cdots + \alpha_i a_i$ with $\alpha_1, \ldots, \alpha_i \in C$ yields $\alpha_i h_i$. If $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ are such that $\alpha_1 a_1 + \cdots + \alpha_m a_m = 0$, then $\alpha_1 = \cdots = \alpha_m = 0$, because if not all of them are zero, let i be maximal with $\alpha_i \neq 0$ and apply $(v_{i-1}S - u_{i-1}) \cdots (v_1 S - u_1)$ to obtain $\alpha_i h_i = 0$, which forces $\alpha_i = 0$.

Section 3.1

1. Differentiating the differential equation leads to a differential equation of order 2, to which the proof given in the text applies.

2. As in the proof of Theorem 3.1, write the differential equation in the form

$$f^{(r)}(x) = g(x) - \frac{p_0(x)}{p_r(x)} f(x) - \cdots - \frac{p_{r-1}(x)}{p_r(x)} f^{(r-1)}(x).$$

By the assumption $p_r(0) \neq 0$, the rational functions on the right hand side can be expanded as power series, say $-\frac{p_i(x)}{p_r(x)} = \sum_{n=0}^{\infty} b_{i,n} x^n$ for certain $b_{i,n} \in C$. Using $f^{(i)}(x) = \sum_{n=0}^{\infty} a_{n+i}(n+i)^{\underline{i}} x^n$ $(i = 0, \dots, r)$ and writing $g(x) = \sum_{n=0}^{\infty} c_n x^n$, we can equate coefficients on both sides of the equation and obtain the recurrence $(n+r)^{\underline{r}} a_{n+r} = c_n + \sum_{i=0}^{r-1} \sum_{k=0}^{n} a_{k+i}(k+i)^{\underline{i}} b_{i,n-k}$ $(n \in \mathbb{N})$. For every choice of initial values $a_0, \dots, a_{r-1}$, this recurrence has a unique infinite sequence solution $(a_n)_{n=0}^{\infty}$. For any such solution, the series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ is a solution of the inhomogeneous differential equation.

3. Consider the coefficient sequence $(a_n)_{n=0}^{\infty}$ of the series. We have $a_n = 1$ if n is a power of two, and $a_n = 0$ otherwise. If the series were D-finite, then by Theorem 3.5, the coefficient sequence would satisfy a recurrence, say $p_0(n)a_n + \cdots + p_r(n)a_{n+r} = 0$ for some polynomials $p_0, \dots, p_r \in C[x]$ with $p_r \neq 0$. For all sufficiently large $k \in \mathbb{N}$, we have $2^k - 2^{k-1} > r$, and in order to have $a_{2^k} = 1$ for these k, we need to have $p_r(2^k - r) = 0$. But the nonzero polynomial p_r can only have finitely many roots.

4. $a_n + (4+n)a_{n+1} + (2+n)(3+n)a_{n+2} + (2+n)(3+n)a_{n+3} = 0$.

5. There are no roots, so we can choose ϕ as small as we like. Let us take $\phi = 1/10$. We have $b_{0,n} = -\delta_{0,n}$ and $b_{1,n} = 2\delta_{0,n}$, so we can take $M = 2$ and $n_0 = 0$. The sum expression

$$\sum_{i=0}^{r-1} \left(\frac{1}{i+1} \frac{(n+i+1)^{\underline{i+1}}}{(n+r)^{\underline{r}}} + (n_0+1)M \frac{(n+i)^{\underline{i}}}{(n+r)^{\underline{r}}} \right) = \frac{n+7}{2(n+2)}$$

is bounded by 1 for $n \geq 3$, so we take $n_1 = 3$. Then $c = \max_{i=0}^{n_1+r-1} |a_i|/\phi^i = \frac{1250}{3}$. We need to find K such that $\frac{c}{(1-|\phi\xi|)} |\phi\xi|^K < 10^{-101}$. A possible choice is $K = 104$. We obtain

$$\mathrm{e} \approx \sum_{n=0}^{104} \frac{1}{n!} = \frac{55991(156\text{ digits suppressed})53293}{20598(156\text{ digits suppressed})00000}$$
$$\approx 2.7182818(84\text{ digits suppressed})25166427.$$

In this example, the approximation is in fact accurate to 169 digits.

6. $p_2(x,y) = x^2(1-y)^2 - x(3y-1)(y-1) + 2y^2$, $p_3(x,y) = x^3(1-y)^3 + 3x^2(2y-1)(y-1)^2 - x(11y^2-7y+2)(y-1) + 6y^3$, $p_4(x,y) = x^4(1-y)^4 - 2x^3(5y-3)(y-1)^3 + x^2(35y^2-34y+11)(y-1)^2 - 2x(25y^3-23y^2+13y-3)(y-1) + 24y^4$.

7. **a.** $(n+1)a_{n+1} - a_n = 0$; **b.** $(n+1)a_{n+1} - (n+1)a_n = 0$; **c.** $(n+3)(n+5)^2 a_n = 0$.

8. We have $\sum_{n=0}^{\infty} a_n(\xi_0 + x)^n = \sum_{n=0}^{\infty} a_n \sum_{k=0}^{\infty} \binom{n}{k} x^k \xi_0^{n-k} = \sum_{k=0}^{\infty} \left(\sum_{n=0}^{\infty} \binom{n}{k} a_n \xi_0^{n-k} \right) x^k$, therefore

$$|b_k| \leq \sum_{n=0}^{\infty} \binom{n}{k} |a_n| |\xi_0|^{n-k} \leq c \sum_{n=0}^{\infty} \binom{n}{k} |\phi\xi_0|^n |\xi_0|^{-k} = \frac{c|\phi|^k}{(1 - |\phi\xi_0|)^{k+1}}$$

for all $k \in \mathbb{N}$ and we can take $\bar{c} = \frac{c}{1-|\phi\xi|}$ and $\bar{\phi} = \frac{\phi}{1-|\phi\xi|}$.

9. It suffices to observe that π is the value of a D-finite function. This is definitely the case. For example, we have $\pi = 4\arctan(1)$, and $f(x) = 4\arctan(x)$ is D-finite, because it satisfies the differential equation $(x^2 + 1) f''(x) + 2x f(x) = 0$.

10. The series about $2/5$ can be truncated after 131 terms. For its initial values, we should seek at least 56 decimal digits to account for error propagation. These initial values can then be computed by truncating the series about 0 after 139 terms. Note that $131 + 139 < 100 + 200$, so $2/5$ is slightly better than $1/2$.

11. 1.0986122886681096913952452369225257046474905578227

12. **a.** $0 - \mathrm{i}$. In this example, it only matters in which sense we bend around the point -1 but not how we bend around $-4/3$ because the latter is a so-called apparent singularity (cf. Definition 3.17). **b.** -1.

13. For a path γ starting at 0, winding around the point -1 in the mathematically positive sense, and then returning to 0, we find the transition matrix

$$T_{0 \xrightarrow{\gamma} 0} \approx \begin{pmatrix} -48.8703 - 31.91368\mathrm{i} & 62.81513 \\ -54.2192 & 48.8703 - 31.91368\mathrm{i} \end{pmatrix}.$$

Its two eigenvalues are near .01976i and 50.607i, so they are definitely not roots of unity. The claim follows.

14. 0.49137867984399145546081755621333943869910921358062.

15. $2c\epsilon|\phi|/(1 - |\phi\bar{\zeta}|)^3$.

16. This case can be handled analogously to the endpoint. Choose a sequence $\zeta_0^{(0)}, \zeta_0^{(1)}, \ldots$ rapidly converging to the startpoint ζ_0 and replace the segment $\zeta_0 - \zeta_1$ by the $M + 1$ segments $\zeta_0^{(M)} - \zeta_0^{(M-1)} - \cdots - \zeta_0^{(0)} - \zeta_1$, for a sufficiently large M.

17. The singular values of a parametrized matrix depend continuously on the parameters. Therefore, since the sequence $(\zeta_s^{(k)})_{k=0}^{\infty}$ is chosen such as to converge to ζ_s and avoids singular points, the corresponding sequence of largest singular values also converges to a limit.

18. 500 terms are enough.

Section 3.2

1. Using $f(x) = g(1/x)$, the hint is easily confirmed by induction on i. For $i = 0$ it follows directly from the definition of $a_{i,j}$, and for $i = 1$ it follows directly from the chain rule $g(1/x)' = g'(1/x)(-1/x^2)$. Now suppose it holds for some $i \geq 1$. Then

$$\begin{aligned} f^{(i+1)}(x) = f^{(i)}(x)' &= (-1)^i \sum_{j=1}^{i} a_{j,i}\bigl(g^{(j)}(1/x)x^{-(i+j)}\bigr)' \\ &= (-1)^i \sum_{j=1}^{i} a_{j,i}\bigl(-g^{(j+1)}(1/x)x^{-(i+j+2)} - (i+j)g^{(j)}(1/x)x^{-(i+j+1)}\bigr) \\ &= (-1)^{i+1}\Biggl(\sum_{j=1}^{i}\bigl(a_{j-1,i} + (i+j)a_{j,i}\bigr)g^{(j)}(1/x)x^{-(i+j+1)} \\ &\qquad + a_{i,i}g^{(i+1)}(1/x)x^{-(2i+2)}\Biggr), \end{aligned}$$

and it just remains to check that $a_{j-1,i} + (i+j)a_{j,i} = a_{j,i+1}$ for all $i, j \geq 1$ and $a_{i,i} = a_{i+1,i+1}$ for all $i \geq 1$, which is routine.

Using the formula from the hint, the differential equation for f becomes

$$\begin{aligned} 0 = \sum_{i=0}^{r} p_i(x)f^{(i)}(x) &= \sum_{i=0}^{r} p_i(x)(-1)^i \sum_{j=0}^{i} a_{j,i}g^{(j)}(1/x)x^{-(i+j)} \\ &= \sum_{j=0}^{r}\Biggl(\sum_{i=j}^{r} p_i(x)(-1)^i a_{j,i}x^{-(i+j)}\Biggr)g^{(j)}(1/x). \end{aligned}$$

Exchange i and j and replace x with $1/x$ to obtain the desired result.

2. $\{x^2 - 2x^3 + 2x^4 + 2x^5 - \frac{27}{4}x^6 + \frac{371}{50}x^7 - \frac{953}{450}x^8 - \frac{6179}{3150}x^9 + \cdots\}$.

3. $\{x^{-2} + \frac{1}{2}x^{-1} - \frac{1}{8} - \frac{31}{16}x - \frac{85}{128}x^2 + \frac{1631}{6400}x^3 + \cdots\}$.

4. $\{x^{-2} + x^{-4} + 9x^{-6} + \frac{73}{9}x^{-8} + \frac{827}{45}x^{-10} + \cdots, x^{-5} - \frac{1}{2}x^{-7} + \frac{57}{56}x^{-9} + \cdots\}$.

5. Every meromorphic function admits a series expansion in $\mathbb{C}((x))$. The solution space of $x^2y'' + (3x-1)y' + y = 0$ in $\mathbb{C}((x))$ is generated by $\sum_{n=0}^{\infty} n!x^n$, which is an element of $\mathbb{C}[[x]]$ but for lack of convergence does not correspond to a meromorphic function. Therefore, this equation has more solutions in $\mathbb{C}[[x]]$ than in $\mathfrak{M}$.

6. We have $(x^\alpha)^{(j)} = \alpha^{\underline{j}}x^{\alpha-j}$ for all $\alpha \in \mathbb{Q}$ and all $j \in \mathbb{N}$. Make an ansatz $p_0y + p_1xy' + \cdots + p_rx^ry^{(r)} = 0$ for a linear differential equation of order r with undetermined constants $p_0, \ldots, p_r$. Setting x^α into the equation yields the requirement $(p_0 + p_1\alpha + \cdots + p_r\alpha^{\underline{r}})x^\alpha = 0$. Taking r different α's yields a system of r linear equations for the $r+1$ unknowns $p_0, \ldots, p_r$. This system must have a nontrivial solution. The solution corresponds to a differential equation with the desired solutions $x^{\alpha_1}, \ldots, x^{\alpha_r}$. As these are linearly independent over C, it is clear that the equation cannot have lower order than r, i.e., we must have $p_r \neq 0$.

7. Since $\sqrt{\sin(x)} = x^{1/2} - \frac{1}{12}x^{5/2} + \frac{1}{1440}x^{9/2} + \cdots$ is not a power series, a differential equation for $\sqrt{\sin(x)}$ would have to have 0 as a singularity. By the periodicity of sin, it would in fact have to have $2n\pi$ as singularity, for every $n \in \mathbb{Z}$. These are infinitely many, but any equation can have at most finitely many singularities, since its singularities are the roots of a polynomial.

8. An equation $p_0 y = 0$ of order zero can only have the zero solution, as follows immediately upon dividing by $p_0 \neq 0$. Consider an equation $y' = py$ of order 1, with $p \in K$, and let $y_1, y_2 \in E$ be two nonzero solutions. Then $y_1' = py_1$, $y_2' = py_2$ implies $(y_1/y_2)' = (y_1' y_2 - y_1 y_2')/y_2^2 = (py_1y_2 - py_1y_2)/y_2^2 = 0$, so y_1, y_2 are linearly dependent over $\mathrm{Const}(K)$, as claimed.

9. **a.** By the product rule, we have $0 = D(1) = D(a/a) = D(a)/a + aD(1/a)$. The claim follows. **b.** For $n = 0$, $D(a^0) = D(1) = 0 = 0a^{-1}D(a)$ follows from the fact that 1 is always a constant. For $n > 0$, the product rule gives $D(a^n) = D(a^{n-1}a) = D(a^{n-1})a + a^{n-1}D(a)$, so the claim follows by induction. For $n < 0$, we have $D(a^n) = D(1/a^{-n}) = -D(a^{-n})/a^{-2n} = -(-n)a^{-n-1}D(a)/a^{-2n} = na^nD(n)$, using part a. **c.** $D(a^nb^m) = D(a^n)b^m + a^nD(b^m) = na^{n-1}b^mD(a) + ma^nb^{m-1}D(b)$. Dividing by a^nb^m gives the result.

10. Since D is additive, it suffices to consider the case $p = ax^n$ for some $n \in \mathbb{N}$ and some $a \in R$. By the product rule, we have $D(au^n) = D(a)u^n + nau^{n-1}D(u)$, as required.

11. We need to solve the differential equation $D(y) = 0$ for y. First, for $p/q \in C(x)$ we have $D(p/q) = (D(p)q - pD(q))/q^2 = 0$ if and only if $D(p)q = pD(q)$. If we assume, as we may, that p and q are coprime, then any irreducible factor of p appears on the right hand side with a higher multiplicity than on the left hand side, and any irreducible factor of q appears on the left hand side with higher multiplicity than on the right hand side. As this is impossible, neither p nor q can have a nontrivial irreducible factor, so every solution of $D(y) = 0$ in $C(x)$ is in fact in C.

For $p = \sum_{n=0}^{\infty} a_nx^n$ we have $D(p) = \sum_{n=0}^{\infty} a_nnx^{n-1}$, which is only zero if $a_n = 0$ for all $n \geq 0$, so again the constant field is C.

12. $C(x/y)$.

13. $D(1) = D(1 \cdot 1) = D(1)1 + 1D(1) = 2D(1) \Rightarrow D(1) = 0 \Rightarrow 1 \in \mathrm{Const}(K)$. Since $\mathbb{Q}$ has no subfields, the claim follows.

14. False, because $D(uv) = -(uv)'' = -u''v - 2u'v' - uv''$ and $D(u)v + uD(v) = -u''v - uv''$ do not agree for all $u, v \in C[x]$.

15. Define $D\colon R[x] \to R[x]$ by $D(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} D(a_k)x^k + \sum_{k=0}^{n} a_k k x^{k-1} u$. Then D is a derivation, $D(x) = u$ and D agrees with the given derivation on R.

16. For every $u \in J$ we have $a^n u = 0$ for some $n \in \mathbb{N}$, so $0 = D(a^n u) = n a^{n-1} D(a)u + a^n D(u) = a^{n-1}(nD(a)u + aD(u))$, so $nD(a)u + aD(u) \in J$, so $aD(u) \in J$ (because $u \in J$), so $D(u) \in J$.

17. In the extension field we have $u(x) = 0$. For any extension of D to the extension field, we must have $D(u(x)) = D(0) = 0$, which forces $(\frac{d}{dx}u)D(x) + \delta_D(u) = 0$, so $D(x) = -\delta_D(u)/(\frac{d}{dx}u)$, where δ_D is the function which applies D to the coefficients of u. Since u is irreducible and $\frac{d}{dx}u$ has smaller degree than u, the quotient $-\delta_D(u)/(\frac{d}{dx}u)$ is well defined as element of $K[x]/\langle u\rangle$. It is equivalent mod $\langle u\rangle$ to a certain polynomial $v \in K[x]$. By the previous exercise, there is a unique extension of D to a derivation on $K[x]$ such that $D(x) = v$. This turns $K[x]$ into a differential ring for which the ideal $\langle u\rangle$ is a differential ideal. Therefore, by part 1 of Lemma 3.21 we obtain that $K[x]/\langle u\rangle$ is a differential field. This shows the existence. The uniqueness follows because the requirement $D(u) = 0$ leaves no other choice for v.

18. **a.** We have $D^i(\exp(\xi x)) = \xi^i \exp(\xi x)$ for all $i \in \mathbb{N}$ and all $\xi \in C$. The claim follows. **b.** The polynomial $14+32x-7x^2-6x^3+x^4$ factors into $(x^2-4x-14)(x^2-2x-1)$ and thus has the roots $2 \pm 3\sqrt{2}$ and $1 \pm \sqrt{2}$. The Picard-Vessiot-extension is therefore $E = C(\exp(x), \exp(\sqrt{2}x))$.

19. If $y \in R_1$ is such that $p_0 y + \cdots + p_r y^{(r)} = 0$, then $\phi(p_0 y + \cdots + p_r y^{(r)}) = 0$, so $\phi(p_0)\phi(y) + \cdots + \phi(p_r)\phi(y)^{(r)} = 0$, so $p_0\phi(y) + \cdots + p_r\phi(y)^{(r)} = 0$, as required.

20. When we conclude from $nu^{n-1}D(u) = 0$ that $D(u)$ is zero divisor. This is only legal step if the positive integer n, interpreted as element of R, is not zero.

21. $\{\sum_{n=-\infty}^{\infty} x^n, (1-x)^{-1}\exp(-x)\}$.

22. We have $U = U_{-2} \times U_2$, where U_ξ is the field of meromorphic functions defined on $B_\xi(1)$. The solution space in each U_ξ contains the exponential function, and since each U_ξ is a differential field, the solution space can have at most dimension 1.

Each solution in U can be viewed as a pair (f_{-2}, f_2) of meromorphic functions, one defined on $B_{-2}(1)$ and the other defined on $B_2(1)$. A basis of the solution space in U is therefore given by $\{(0, \exp), (\exp, 0)\}$. The solution space has dimension 2. This result is not in conflict with Theorem 3.20, because U is not an integral domain.

23. $D(y_1 - y_2 - y_3) = D(uv)/(uv) - D(u)/u - D(v)/v = \frac{D(u)v - uD(v)}{uv} - \frac{D(u)}{u} - \frac{D(v)}{v} = 0.$

Section 3.3

1. Obvious.

2. By applying the substitution $t = \exp(u)$, we find that $\int \frac{1}{\log(t)} dt = \int \frac{\exp(u)}{u} du$. The latter is D-finite because $\exp(u)/u$ is and integration preserves D-finiteness. Up to constants of integration (which don't matter here), we have $\mathrm{li}(t) = f(\log(t))$ where $f(u) = \int \frac{\exp(u)}{u} du$ is D-finite. It follows that $\mathrm{li}(\exp(z)) = f(z)$ is D-finite.

3. By definition of F, the left hand side satisfies the differential equation $(x-1)xf'' + (ax + bx - 2b + x)f' + abf = 0$. For the right hand side, start from the differential equation $4(x-1)xf'' - 2(-2ax+2b-3x+1)f' + a(a+1)f = 0$, which has $F(\frac{a}{2}, \frac{a+1}{2}; b + \frac{1}{2}; x)$ as a solution. Applying the closure property algorithm for substitution of algebraic functions yields the equation $(x-1)x(x-2)^2 f'' + (x-2)(-ax^2 + bx^2 - 4bx + 4b + x^2 - 2x)f' + a(a+1)xf = 0$, which has $F(\frac{a}{2}, \frac{a+1}{2}; b+\frac{1}{2}; x^2/(2-x)^2)$ as a solution. Applying the closure property algorithm for multiplication to this equation and the equation $(x-2)f' + af = 0$ satisfied by $(1 - \frac{x}{2})^{-a}$ yields the equation stated at the beginning for the left hand side. Since both sides are power series and the equation only has a one-dimensional solution space in $C[[x]]$, we can conclude the proof by observing that both sides are equal to 1 for $x = 0$.

4. Considering ν as a (formal) parameter, we have three functions $J_{\nu+2}(x), J_{\nu+1}(x), J_\nu(x)$ satisfying the differential equations $x^2 J''_{\nu+2}(x) + xJ'_{\nu+2}(x) + (x^2 - (\nu+2)^2)J_{\nu+2}(x) = 0$, $x^2 J''_{\nu+1}(x) + xJ'_{\nu+1}(x) + (x^2 - (\nu+1)^2)J_{\nu+1}(x) = 0$, and $x^2 J''_\nu(x) + xJ'_\nu(x) + (x^2 - \nu^2)J_\nu(x) = 0$. From the last equation and the equation $xf' - f = 0$ satisfied by x, we get that $xJ''_\nu(x)$ satisfies the equation $x^2 f'' - xf' + (1 - \nu^2 + x^2)f = 0$. Replacing ν by $\nu + 2$ gives an equation for $xJ''_{\nu+2}(x)$. Now applying the closure property algorithm for addition yields the equation

$$x^4 f^{(4)} + 2x^3 f^{(3)} + x^2(-2\nu^2 - 4\nu + 2x^2 - 3)f'' \\ + x(2\nu^2 + 4\nu + 2x^2 + 3)f' + (\nu^2 - x^2 - 1)(\nu^2 + 4\nu - x^2 + 3)f = 0$$

which has $f = xJ_{\nu+2}(x) - 2(\nu+1)J_{\nu+1}(x) + xJ_\nu(x)$ as a solution. Using the initial values for $J_\nu, J_{\nu+1}, J_{\nu+2}$, we can verify that $f = 0x^\nu + 0x^{\nu+1} + 0x^{\nu+2} + 0x^{\nu+3} + \cdots \in \mathbb{C}[[x]]$. Since the differential equation derived for f only admits solutions in $\mathbb{C}[[x]]$ with starting exponents $\nu + 1$ and $\nu + 3$, it follows that $f = 0$.

5. For $h = f+g$ we have $(2x^5 - 11x^4 - 38x^3 - 38x^2 - 15x - 2)h^{(4)} + (7x^5 - 34x^4 - 180x^3 - 223x^2 - 100x - 13)h^{(3)} + (9x^5 - 44x^4 - 263x^3 - 354x^2 - 175x - 19)h'' + (5x^5 - 27x^4 - 153x^3 - 209x^2 - 104x - 10)h' + (x^5 - 6x^4 - 32x^3 - 40x^2 - 14x - 2)h = 0$. For $h = fg$ we have $(4x^8 - 172x^7 - 911x^6 - 1948x^5 - 2256x^4 - 1540x^3 - 622x^2 - 138x - 13)h^{(4)} + (28x^8 - 1194x^7 - 7012x^6 - 16288x^5 - 20242x^4 - 14710x^3 - 6298x^2 - 1480x - 148)h^{(3)} + (73x^8 - 3110x^7 - 18928x^6 - 45411x^5 -$

$58169x^4 - 43532x^3 - 19210x^2 - 4669x - 486)h'' + (84x^8 - 3603x^7 - 21297x^6 - 49955x^5 - 62936x^4 - 46493x^3 - 20289x^2 - 4889x - 508)h' + (36x^8 - 1569x^7 - 8237x^6 - 18779x^5 - 23959x^4 - 18249x^3 - 8292x^2 - 2099x - 231)h = 0.$

6. The equation constructed by the algorithm is the lowest order differential equation which annihilates $\alpha x^2 + \beta x^3$ for all constants α, β. The first order equation works only for some particular choices of α, β.

7. For $h = \int f$ we have $(x+2)h''' + (3x+4)h'' + (5x+6)h' = 0$. For $h = f'$ we have $(5x^2 + 16x + 12)h'' + (15x^2 + 38x + 20)h' + (25x^2 + 60x + 34)h = 0$. For $h(x) = f(x/(1-x))$ we have $(x^5 - 6x^4 + 14x^3 - 16x^2 + 9x - 2)h''(x) + (2x^4 - 9x^3 + 12x^2 - 5x)h'(x) + (x-6)h(x) = 0$.

8. We proceed as in the proof of Theorem 2.30 to construct a differential equation satisfied by all a_i. We write the differential equation for a_i as $\sum_{j=0}^{r_i} p_{i,j} D^j(a_i) = 0$ with $p_{i,j} \in C[x]$ of degree at most d_i, set $r = \sum_{i=1}^{m} r_i$, and make an ansatz $\sum_{k=0}^{r-r_i} q_{k,i} D^k(\sum_{j=0}^{r_i} p_{i,j} D^j(a_i)) = 0$ for unknown polynomials $q_{k,i}$. Expanding the ansatz and equating the coefficients of corresponding terms $D^j(a_i), D^j(a_{i'})$ leads to a linear system with $m(r+1) - r$ variables (the $q_{k,i}$) and $(m-1)(r+1)$ equations (one for every $i = 2, \ldots, m$ and every $j = 0, \ldots, r$). Since $m(r+1) - r - (m-1)(r+1) = 1 > 0$, this system has a nontrivial solution. For every $i = 1, \ldots, m$, the matrix of the linear system has $r + 1 - r_i$ columns with entries of degree at most d_i. By Theorem 1.29, there is a solution vector with polynomial coefficients with the property that for any k such that the kth column of the matrix has entries of degree at most d_i, the kth component of the solution vector has degree at most $\sum_{j=1}^{m} d_j(r+1-r_j) - d_i$. Therefore, plugging the coordinates of the solution vector into the ansatz for the ith differential equation (for any i) leads to an equation matching the claimed degree bound.

9. Addition should lead to differential equations of order $r_a + r_b$ and degree $(r_a + 1)d_b + (r_b + 1)d_a$, as stated in the theorem. Multiplication should lead to differential equations of order $r_a r_b$ and degree $(r_a d_b + r_b d_a)(r_a r_b - r_a - r_b + 2)$. The degree bound stated in the theorem seems to overshoot slightly.

10. False. All generators of the Picard-Vessiot-extension are D-finite by definition, and D-finiteness is preserved by addition and multiplication. However, the quotient of two D-finite functions is in general not D-finite. An example is $\tan(x)$ (cf. Exercise 2 of Sect. 1.2).

11. The solution space of the given differential equation in $C[[x+4]]$ is generated by

$$1 - \tfrac{1}{6}(x+4) + \tfrac{1}{1296}(x+4)^2 + \tfrac{11}{31104}(x+4)^4 + \cdots$$
$$\text{and} \quad (x+4)^2 + \tfrac{2}{9}(x+4)^3 + \tfrac{13}{216}(x+4)^4 + \cdots$$

We have added $x = -4 + (x+4) \in C[[x]]$ to the solution space. By taking suitable C-linear combinations of these three series, we can obtain series of the form $1+\cdots$, $(x+4)+\cdots$, and $(x+4)^2+\cdots$. This is the reason.

12. The starting exponents of the given power series solutions of A and B are 0 and 1, so these equations have no singularity at 0. The power series solutions of C are linear combinations of solutions of A or B. We can determine the starting exponents by writing the given parts of the coefficient sequences into the rows of a matrix and compute a triangular form:

$$\begin{pmatrix} 1 & 3 & 7 & -2 & 3 \\ 0 & 1 & 2 & -9/5 & 2 \\ 1 & -1 & -1 & 3 & -1 \\ 0 & 1 & 2 & -5 & -1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We see that the starting exponents are $0, 1, 3, 4$. The claim follows because 2 is missing.

13. f is D-finite, so the vector space generated by f, $D(f)$, $D^2(f), \ldots$ in F over K has finite dimension. Then also the subspace generated by $D(f)$, $D^2(f), \ldots$ has finite dimension. This implies that $D(f)$ is D-finite.

14. Let $\{b_1, \ldots, b_d\}$ be a basis of K over $C(x)$. We can write the differential equation for f in the form $\sum_{i=0}^{r}\sum_{j=0}^{d-1} a_{i,j} b_j f^{(i)} = 0$ for certain $a_{i,j} \in C(x)$. Consider a K-linear combination of the first $(d-1)r$ derivatives of this equation with undetermined coefficients $u_0, \ldots, u_{(d-1)r} \in K$ Each u_i has the form $\sum_{j=0}^{d-1} u_{i,j} b_j$ for certain (for the moment unknown) $u_{i,j} \in C(x)$. The new equation for f has the form $\sum_{i=0}^{dr}\sum_{j=0}^{d-1} q_{i,j} b_j f^{(i)} = 0$ for certain $q_{i,j}$ which are $C(x)$-linear combinations of the unknown coefficients $u_{i,j}$. Equating all coefficients of $b_2, \ldots, b_d$ to zero gives a linear system over $C(x)$ with $((d-1)r+1)d$ variables $u_{i,j}$ and $(dr+1)(d-1)$ equations (one for each term $b_j f^{(i)}$ in the enlarged equation). Because of $((d-1)r+1)d > (dr+1)(d-1)$, the system has a nontrivial solution. Dividing the corresponding equation by b_1 gives an equation of order $\leq dr$ with coefficients in $C(x)$.

It remains to show that this equation is not identically zero. To see that this is the case, let i_0 be maximal such that $\sum_{j=0}^{d-1} a_{i_0,j} b_j \neq 0$ and let i_1 be maximal such that $\sum_{j=0}^{d-1} u_{i_1,j} b_j \neq 0$. Then the coefficient of $f^{(i_0+i_1)}$ in the output equation is $(\sum_{j=0}^{d-1} a_{i_0,j} b_j)(\sum_{j=0}^{d-1} u_{i_1,j} b_j) \neq 0$.

15. Use the differential equation to get many more coefficients of f, then guess an algebraic equation. This should give the conjecture $(-16x^2 - 32x - 16) f(x)^4 + (8x^3 - 8x^2 - 8x + 8) f(x)^2 + (-8x^4 - 16x^3 + 16x + 8) f(x) + (x^5 + 4x^4 + 14x^3 + 4x^2 + 9x) = 0$. To prove that this equation is correct, define g as the left hand side and use closure properties to compute a differential equation for g. This should give a differential equation of order 5 which does not have 0 as singularity. Therefore,

$g = 0 \iff g(0) = \cdots = g^{(4)}(0) = 0$, which can easily be checked using the coefficients of f.

16. In order to see that there is a unique power series solution, write the equation in the form $f'(x) = -\frac{2x}{2x-1} f(x) + \exp(x)\frac{x+1}{2x-1} f(x)^2$. Setting $f(x) = \sum_{n=0}^{\infty} a_n x^n$ for undetermined a_n into the equation and extracting the coefficient of x^n on both sides, we get $(n+1)a_{n+1}$ from the left hand side, and on the right hand side some complicated expression which however only depends on $a_0, \dots, a_n$. Therefore, the given partial solution admits a unique extension to an infinite series solution.

In order to see that this solution is D-finite, compute many more coefficients and then guess a differential equation. This should lead to the conjecture $(x+1)(2x-1)(x^2+14x-5)f''(x)+(4x^4+65x^3+54x^2+19x-28)f'(x)+2(x^4+18x^3+27x^2+22x-6)f(x) = 0$. To prove that this equation is correct, let g be a solution of the conjectured differential equation with $g(0) = 1$, $g'(0) = 1$. Use closure properties to compute a differential equation for $h(x) = 2xg(x)+\exp(x)(x+1)g(x)^2+(2x-1)g'(x)$. This should give a differential equation of order 5 which does not have 0 as a singularity. Therefore, $h = 0 \iff h(0) = \cdots = h^{(4)}(0) = 0$, which can be easily checked using the coefficients of g.

17. For example, $\exp(\exp(x))$ is not. If it were, then $\exp(x)$ would be algebraic. To see this, set $f(x) = \exp(\exp(x))$ and note that $f^{(k)}(x) = f(x)P_k(\exp(x))$ for some polynomial $P_k \in C[y]$ of degree k. Any nontrivial differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ would give rise to a nontrivial algebraic equation $p_0(x)P_0(\exp(x)) + \cdots + p_r(x)P_r(\exp(x)) = 0$ for $\exp(x)$.

18. For example, $1/\log(x)$ is not. To see this, set $f = 1/\log(x)$ and observe that $f^{(k)} = \frac{1}{x^k} P_k(1/\log(x))$ for some polynomial $P_k \in C[x]$ of degree $k+1$. Thus any differential equation $p_0 f + \cdots + p_r f^{(r)} = 0$ would give rise to a polynomial equation for $\log(x)$, in contradiction to the logarithm being transcendental.

19. For example, $\exp(1/x)$ is D-finite but its functional inverse $1/\log(x)$ is not, by the previous exercise.

20. If f and g are D-finite, so are $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ by Theorem 3.5. Then $(a_n b_n)_{n=0}^{\infty}$ is D-finite by Theorem 2.30. The claim follows via Theorem 2.33.

21. If $\log(\log(x))$ is D-finite, then so is its derivative $\frac{1}{x\log(x)}$, but then also $\frac{1}{\log(x)}$, a contradiction.

If $\sqrt{\log(x)}$ is D-finite, then so is its derivative $\frac{1}{2x\sqrt{\log(x)}}$, and then so is the square of this function, $\frac{1}{4x^2\log(x)}$, and then also $1/\log(x)$, a contradiction.

22. Write $y = f'/f$. Then $K = C(x)(y)$ is a differential field and a $C(x)$-vector space of finite dimension r. For any $a \in K$ we have $(fa)' = f'a + fa' = f(ya + a')$. Therefore, $f, f', f'', \dots$ all are K-multiples of f, and therefore, $f, \dots, f^{(r)}$ are linearly dependent over $C(x)$.

Similarly, for any $a \in K$ we have $(a/f)' = (a'f - af')/f^2 = (a' - ay)/f$. Therefore, $1/f, (1/f)', \dots$ all are K-multiples of $1/f$, and therefore, $1/f, \dots, (1/f)^{(r)}$ are linearly dependent over $C(x)$.

Section 3.4

1. For each fixed j, the polynomials $(\frac{x+j}{v})^{\underline{i}}$ for $i = 0, \ldots, r$ are linearly independent over C, so if $p_j = 0$, then $p_{i,d+vi-j} = 0$ for $i = 0, \ldots, r$. By assumption of the definition, $p_r \neq 0$, so in particular not all coefficients $p_{i,k}$ are zero. If (i, k) is such that $p_{i,k} \neq 0$, set $j = d + vi - k$. Then $p_{i,d+vi-j} \neq 0$, so $p_j \neq 0$ for this choice j. This shows that indices j with $p_j \neq 0$ exist. To see that there is a maximal such index, observe that every j with $p_j \neq 0$ must be an integer and that $p_j = 0$ whenever $j > d + vr$.

2. $q_{vr+d} = \sum_{i=0}^{r} p_{i,d+vi-(vr+d)}(\frac{x+j}{v})^{\underline{i}} = \sum_{i=0}^{r} p_{i,v(i-r)}(\frac{x+j}{v})^{\underline{i}} = p_{r,0}(\frac{x+j}{v})^{\underline{r}}$, because we have $p_{i,v(i-r)} = 0$ when $i < r$. By definition of ordinary points, 0 is an ordinary point if and only if $p_{r,0} \neq 0$. By definition of the indicial polynomial, $\eta = q_{vr+d}$ if and only if this is nonzero, which by the above computation is equivalent to $p_{r,0} \neq 0$.

3. Writing $L = \sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} p_{i,j} x^{j/v} D^i$ for certain $p_{i,j} \in C$ with $p_{i,j} = 0$ for $j < 0$ or $j > d$, we have

$$x^{-q/v+r}(L \cdot x^{q/v}) = x^{-q/v+r} \sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} p_{i,j} x^{j/v} (q/v)^{\underline{i}} x^{q/v-i}$$
$$= \sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} p_{i,j} (q/v)^{\underline{i}} x^{j/v+r-i}.$$

Since $i \leq r$, it is clear that this belongs to $C[q][x^{1/v}]$. Substituting $j = d + vi - k$, we further get

$$\ldots = \sum_{i=0}^{r} \sum_{k\in\mathbb{Z}} p_{i,d+vi-k} (q/v)^{\underline{i}} x^{(d+k)/v+r}$$
$$= \sum_{k\in\mathbb{Z}} \Bigl(\sum_{i=0}^{r} p_{i,d+vi-k} (q/v)^{\underline{i}} \Bigr) x^{(d+k)/v+r}.$$

Comparison with Definition 3.34 completes the proof.

4. Write the differential equation as $\sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} p_{i,j} x^{j/v} f^{(i)}(x) = 0$ with the understanding that $p_{i,j} = 0$ if $j < 0$ or $j > d$. Setting $f(x) = \sum_{n\in\mathbb{Z}} c_n x^{(n+q)/v}$ gives

$$\sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} p_{i,j} x^{j/v} \sum_{n\in\mathbb{Z}} c_n (x^{(n+q)/v})^{(i)} = \sum_{i=0}^{r} \sum_{j\in\mathbb{Z}} \sum_{n\in\mathbb{Z}} p_{i,j} c_n \bigl(\frac{n+q}{v}\bigr)^{\underline{i}} x^{(n+q+j)/v-i}$$

$$\overset{j=d+vi-k}{=} \quad \sum_{i=0}^{r}\sum_{k\in\mathbb{Z}}\sum_{n\in\mathbb{Z}} p_{i,d+vi-k}c_n\Big(\frac{n+q}{v}\Big)^{\underline{i}}x^{(n+d-k+q)/v}$$

$$\overset{n=m-k}{=} \quad \sum_{m\in\mathbb{Z}}\sum_{k\in\mathbb{Z}}\Bigg(\underbrace{\sum_{i=0}^{r} p_{i,d+vi-k}\Big(\frac{(m+k)+q}{v}\Big)^{\underline{i}}}_{=q_k(m+q)}\Bigg)c_{m+k}x^{(m+d+q)/v}.$$

By definition of the c_n, we have $\sum_{k\in\mathbb{Z}} q_k(m+q)c_{m+k} = 0$ for all $m \in \mathbb{Z} \setminus \{-j\}$, where $j \in \mathbb{Z}$ is as in Definition 3.34. Therefore, all coefficients in the above series vanish, except for the coefficient of $x^{(q+d-j)/v}$, which, again by Definition 3.34, is equal to $\eta(q)$.

5. The equation is $105x^3 f^{(3)}(x)+244x^2 f''(x)+49xf'(x)-f(x) = 0$ and can be found by closure properties from equations of the form $xf'(x) - \alpha f(x) = 0$, which have x^α as solution. There is no lower order equation because $x^{1/3} + x^{1/5} + x^{1/7}$ cannot be written as a C-linear combination of two or fewer series in $x^\alpha C[[x]]$. Note that the question requires polynomial coefficients, i.e., $v = 1$.

6. Because of $\log(x^{-1}) = -\log x$, there is no need to make a distinction.

7. The indicial polynomial η must have $\sqrt{2}$ as a root, and since the constant field is $\mathbb{Q}$, this implies $(x^2 - 2) \mid \eta$. Furthermore, because of the logarithm, the multiplicity must be at least two, or η has another root at an integer distance to $\sqrt{2}$. In any case, $\deg \eta$ is at least 4, which implies the claim.

8. False: $x^8 f'(x)+(7+84x^4-9x^6)f(x) = 0$ has the solution $f(x) = \exp(x^{-7} + 28x^{-3} - 9x^{-1})$.

9. **a.** $\mathrm{e}^{\pm 3x^{-1/2}}x^{5/7}(1 + x + x^2 \pm \frac{1}{105}x^{5/2} + \frac{85}{126}x^3 \mp \frac{109}{630}x^{7/2} + \cdots)$; **b.** $x^{3/5}(1 + \frac{1}{4}x + \frac{19}{200}x^2 + \frac{553}{160000}x^3 - \frac{613}{96000000} + \cdots) + x^{18/5}(\frac{1}{48} + \frac{1}{192}x + \frac{187}{96000}x^2 + \cdots)\log(x)$, $x^{18/5}(1 + \frac{1}{4}x + \frac{187}{2000}x^2 + \frac{779}{36000}x^3 + \cdots)$; **c.** $\mathrm{e}^{2x^{-5}-4x^{-4}+5x^{-3}-\frac{33}{5}x^{-2}+\frac{1094}{375}x^{-1}}x^{358892/28125}(1+\frac{10712386}{421875}x+\frac{63816586067498}{177978515625}x^2+\cdots)$, $\mathrm{e}^{2x^{-5}-4x^{-4}+\frac{58}{5}x^{-2}+\frac{5656}{375}x^{-1}}x^{-246392/28125}(1 - \frac{9688636}{421875}x + \frac{41164231171748}{177978515625}x^2 + \cdots)$

10. **a.** $\mathrm{e}^{x^2+2x}x^{-15/14}(1 - \frac{29}{28}x^{-1} + \frac{2553}{1568}x^{-2} - \frac{137055}{43904}x^{-3} + \cdots)$ and $1 + \frac{1}{28}x^{-1} - \frac{87}{1568}x^{-2} + \frac{17515}{43904}x^{-3} + \cdots$; **b.** $\mathrm{e}^{\frac{1}{8}x^2+\frac{1}{2}x}x^{21/25}(1 - \frac{38}{25}x^{-1} + \frac{844}{625}x^{-2} - \frac{387944}{46875}x^{-3} + \cdots)$ and $x^{34/25}(1 - \frac{12}{25}x^{-1} + 4x^{-2} - \frac{256672}{46875}x^{-3} + \cdots)$; **c.** $x(1 - 167x{-}1 - \frac{1067}{2}x^{-2} - \frac{3519}{2}x^{-3} - \frac{26908}{5}x^{-4} + \cdots) - (-18 + \frac{60}{7}x^{-6} - \frac{1395}{49}x^{-7} + \frac{1647}{28}x^{-8} + \cdots)\log(x)$ and $1 - \frac{10}{21}x^{-6} + \frac{155}{98}x^{-7} - \frac{183}{56}x^{-8} + \cdots$.

11. A quick way is to drop the $\cdots$, replace x by $1 - z$, expand the resulting expression as a power series, guess a differential equation from its coefficients, and then undo the change of variables $x = 1 - z$ in the resulting equation. This gives a differential equation of order 3 and degree 13. High degree terms can be dropped because they only affect higher order terms of the solutions. A possible result is the equation $8(11x^4+2x^2-2)x^3f'''(x)-4(363x^4+58x^2-50)x^2f''(x)+2(4235x^4+642x^2-450)xf'(x)-17(935x^4+162x^2-90)f(x)=0$.

12. Suppose that $\sum_{i=0}^r\sum_{j=0}^d p_{i,j}x^j f^{(i)}(x)=0$ with $f(x)=\sum_{k=0}^m f_k(x)\log(x)^k$ for certain $f_k\in C[[x]]$. Clearly, $\sum_{i=0}^r\sum_{j=0}^d p_{i,j}x^j f^{(i)}(x)$ is an element of $C[[x]][\log(x)]$, and as such it is zero iff the coefficient of every power of $\log(x)$ of it is zero. By the product rule, $f^{(i)}(x)=f_m^{(i)}(x)\log(x)^m+\cdots$, where the $\cdots$ only involve logarithms to powers less than m. Consequently,

$$0=[\log(x)^m]\sum_{i=0}^r\sum_{j=0}^d p_{i,j}x^j f^{(i)}(x)=\sum_{i=0}^r\sum_{j=0}^d p_{i,j}x^j[\log(x)^m]f^{(i)}(x)$$

$$=\sum_{i=0}^r\sum_{j=0}^d p_{i,j}x^j f_m^{(i)}(x),$$

as claimed.

13. The term $\exp(-p(x^{-1}))x^{-\alpha}$ is D-finite since it satisfies the equation $x^2f'(x)+(p'(1/x)-\alpha x)f(x)=0$. Since the generalized series solution itself is D-finite, closure properties imply that the series part alone, $a_0(x)+a_1(x)\log(x)+\cdots+a_m(x)\log(x)^m$, is D-finite. By the previous exercise, it follows that $a_m(x)$ is D-finite. Again using closure properties, it follows that $a_m(x)\log(x)^m$ is D-finite, and hence also $a_0(x)+a_1(x)\log(x)+\cdots+a_{m-1}(x)\log(x)^{m-1}$. Repeating the argument m times shows that all a_i are D-finite.

14. Of course: since x^7, x^5 and $\log(x)$ are all D-finite by themselves, it follows from closure properties that $x^7+x^5\log(x)$ is D-finite, so it is a solution of a differential equation. It is true however that whenever there is a solution of the form $x^7(1+\cdots)+x^5\log(x)(1+\cdots)$, then there is also one of the form $x^5(1+\cdots)+x^5\log(x)(1+\cdots)$. This follows from Exercise 12.

15. False: the differential equation $x(x+1)f''(x)-xf'(x)+f(x)=0$ has 0 as a (non-apparent) singular point, but its indicial polynomial is $x(x-1)$.

16. Because of the exponential part and the hint, we expect an equation of the form $p_{2,2}x^2f''(x)+(p_{1,0}+p_{1,1}x+p_{1,2}x^2)f'(x)+(p_{0,0}+p_{0,1}x+p_{0,2}x^2)f(x)=0$. We can plug the known terms into the left hand side and equate coefficients to zero. Note that this gives 7 equations for 6 unknowns, so we are entitled to have some confidence into the solution, if there is one. And indeed there is one: $2x^2f''(x)-(x^2-3x-2)f'(x)+(43x^2+17x-2)f(x)=0$.

17. The Newton polygon consists of a single edge of width 1. This has two consequences. First, the slope can only be an integer, so the exponential part can only contain monomials with integer exponents. Second, once the slope is 1, the indicial polynomial must have degree 1, so it has a single root. Therefore, there can be no logarithms.

18. The Newton polygon of C is $(0,0)-(1,1)-(2,3)-(3,6)$ or $(0,0)-(2,2)-(3,4)-(4,7)$, or a vertically shifted copy of these, and the Newton polygon of D is $(0,0)-(1,1)-(2,3)-(3,8)$, or a vertically shifted copy.

19. Because of linearity, it suffices to consider what happens with a single term $x^{j/v} f^{(i)}(x)$. Applying the substitution and using the product rule turns this term into

$$x^{j/v} \sum_{\ell=0}^{i} \binom{i}{\ell} \exp(sx^{u/v})^{(\ell)} g^{(i-\ell)}.$$

The assertion follows if we can show that the ℓ-th derivative of $\exp(sx^{u/v})$ is a $C[s][x^{1/v}]$-multiple of $\exp(sx^{u/v})$. This follows easily by induction on ℓ, as

$$\big(q(x)\exp(sx^{u/v})\big)' = q'(x)\exp(sx^{u/v}) + q(x)\frac{su}{v}x^{u/v-1}\exp(sx^{u/v})$$

for every $q \in C[s][x^{1/v}]$.

20. If it were, then $x^x = \exp(x\log(x)) = \sum_{n=0}^{\infty} \frac{1}{n!}(x\log(x))^n$ could be identified with a certain linear combination of generalized series as considered in this section. This is not possible because the series considered here can only have bounded degree in $\log(x)$.

21. In the case $n = 1$, the rule $Df = fD + f'$ expresses that multiplication by f followed by differentiation has the same effect as adding the results of multiplication by f' and differentiation followed by multiplication by f. This is true because of the product rule. The case $n > 1$ can be shown by induction using Pascal's triangle.

$$\begin{aligned}
D^n f = DD^{n-1} f = D\sum_{k=0}^{n-1}\binom{n-1}{k} f^{(n-1-k)} D^k &= \sum_{k=0}^{n-1}\binom{n-1}{k} Df^{(n-1-k)} D^k \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}(f^{(n-1-k)}D + f^{(n-1-k+1)})D^k \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k} f^{(n-k)} D^k + \sum_{k=0}^{n-1}\binom{n-1}{k} f^{(n-(k+1))} D^{k+1} \\
&= \sum_{k=0}^{n}\underbrace{(\binom{n-1}{k} + \binom{n-1}{k-1})}_{=\binom{n}{k}} f^{(n-k)} D^k.
\end{aligned}$$

22. $e^{sx^c}x^{\alpha+1}(\frac{1}{\alpha+1} - \frac{cs}{(\alpha+1)(\alpha+1+c)}x^{-c} + \frac{(cs)^2}{(\alpha+1)(\alpha+1+2c)}x^{-2c} - \frac{(cs)^3}{(\alpha+1)(\alpha+1+2c)(\alpha+1+3c)}x^{-3c} + \cdots)$

23. The exponential part originates from an edge of slope $1 + u/p = (p + u)/p$ in the Newton polygon. Because of $v = 1$, the coordinates of the vertices of the Newton polygon are integers. Therefore, an edge with the desired slope must have a width of kp for some positive integer k. This implies the lower bound on the order. For the same reason, the horizontal distance between any two internal vertices of that edge must be an integer multiple of p. This implies that we have $\mu = s^i g(s^p)$ for some polynomial $g \in C[s]$. It follows that whenever σ is a nonzero root of μ, then so is $\omega\sigma$.

24. Here are the singularities together with the corresponding indicial polynomials, their traces, and their defects:

ξ	η	$\mathrm{Tr}(\eta)$	$d(\xi)$
0	$9x(2x-1)$	$1/2$	$-1/2$
1	$-4x(3x-1)$	$1/3$	$-2/3$
3	$36x(x-2)$	2	1
∞	$(2x+1)(3x+1)$	$-5/6$	$1/6$
			sum: 0

25. For every $g \in C(x)$ and every $\xi \in \bar{C}$, the term $\log(g)$ admits an expansion in $\bar{C}[[[x - \xi]]]$. This expansion will involve logarithmic terms if ξ is a root or a pole of g. Therefore, any such ξ must be a singularity of the given equation, and therefore, every solution of the requested type must have the form $\log((x-4)^{e_1}(x-1)^{e_2}(x+1)^{e_3}(x+2)^{e_4})$ for some $e_1, \dots, e_4 \in \mathbb{Z}$. Equivalently, we have to find $e_1, \dots, e_4 \in \mathbb{Z}$ such that $e_1 \log(x-4) + e_2 \log(x-1) + e_3 \log(x+1) + e_4 \log(x+2)$ is a solution. Plugging this ansatz into the equation and equating coefficients of x^k to zero gives a linear system for the e_i whose solution set in $\mathbb{Z}^4$ is generated by $(7, 5, -2, 0)$. Therefore, the only solutions are nonzero constant multiples of $(x-4)^7(x-1)^5/(x+1)^2$ and their integer powers.

26. The generalized series solutions at 0 are $x^{\sqrt{2}}(1 + \frac{1}{2}x + \frac{3}{8}x^2 + \frac{5}{16}x^3 + \cdots)$ and $x^{-\sqrt{2}}(1 + \frac{1}{2}x + \frac{3}{8}x^2 + \frac{5}{16}x^3 + \cdots)$. Since every other series solution must be a linear combination of those two, every nonzero series solution consists of terms with irrational exponents. If there were an algebraic solution, it would have an expansion with rational exponents only.

Section 3.5

1. For $g(x) = f(1/x)$ and $q_i(x) = \sum_{j=i}^{r} p_j(1/x)(-1)^j a_{i,j} x^{i+j}$ and $a_{i,j}$ as in Exercise 1 of Sect. 3.2 we have $\sum_{i=0}^{r} q_i(x) g^{(i)}(x) = 0$. According to Definition 3.48 we have $\eta_\infty = \sum_{i=0}^{r}([x^{k+i}]p_i)x^{\underline{i}}$, with $k \in \mathbb{Z}$ maximal so that this expression is nonzero. According to Definition 3.34, we have $\tilde{\eta}_0 = \sum_{i=0}^{r}([x^{k+i}]q_i)x^{\underline{i}}$, with $k \in \mathbb{Z}$ minimal so that this expression is nonzero.

For any $k \in \mathbb{Z}$ we have

$$\begin{aligned}\sum_{i=0}^{r}([x^{k+i}]q_i)x^{\underline{i}} &= \sum_{i=0}^{r}\Bigg(\sum_{j=i}^{r}(-1)^j a_{i,j}[x^{k+i}]\big(p_j(1/x)x^{i+j}\big)\Bigg)x^{\underline{i}}\\ &= \sum_{i=0}^{r}\Bigg(\sum_{j=i}^{r}(-1)^j a_{i,j}[x^{j-k}]p_j\Bigg)x^{\underline{i}}\\ &= \sum_{j=0}^{r}\Bigg(\sum_{i=0}^{r}(-1)^j a_{i,j}x^{\underline{i}}\Bigg)[x^{j-k}]p_j.\end{aligned}$$

Now a minimal k is clearly the same as a maximal $-k$, so all that remains is to prove the identity $\sum_{i=0}^{j}(-1)^j a_{i,j} x^{\underline{i}} = (-x)^{\underline{j}}$ for $j \in \mathbb{N}$. We can leave this to a computer algebra system.

Finally, the sign change in the argument is because the polynomial η_∞ signals starting exponents with respect to powers of x while the polynomial η_0 signals starting exponents with respect to powers of x^{-1}, and in view of $x^\alpha = (x^{-1})^{-\alpha}$, it is to be expected that roots of one polynomial correspond to negative roots of the other.

2. For example, the following Mathematica code does the job:

```
polysol[eq_, f_[x_]] := Module[{η, n, a, vars, sol},
  η = Last[CoefficientList[Numerator[Together[(eq/.f → (#^n&))/x^n]], x]];
  If[Exponent[η, n] < 1, Return[{}]];
  n = Max[Select[n/.Solve[η == 0, n], IntegerQ]];
  If[n < 0, Return[{}]];
  vars = Table[a[i], {i, 0, n}];
  sol = First[Solve[CoefficientList[eq/.f → Function[x, Sum[a[i]x^i, {i, 0, n}]],
      x] == 0, vars]];
  DeleteCases[Sum[a[i]x^i, {i, 0, n}]/.sol/.Table[{a[i]→1}, {i, 0, n}]/.a[_]
      →0, 0]];
```

3. Bases of the solution spaces are: **a.** $\{1, x, x^2, x^3, x^4\}$; **b.** $\{1495040x + 1576960x^2 + 651840x^3 + 141680x^4 + 17920x^5 + 1344x^6 + 56x^7 + x^8\}$; **c.** $\{x^{99}\}$; **d.** $\{438104268 - 257805009x + 82375425x^2 - 14271675x^3 + 3993660x^4 +$

$127974x^5 + 142758x^6 + 34650x^7 + 715x^9 + 33x^{10} + x^{11}$, $1788185 - 1052304x + 336380x^2 - 58608x^3 + 16830x^4 + 924x^6 + 33x^8\}$

4. If f was a polynomial solution of degree n, the term $(x+\alpha)f(x)$ would be a polynomial of degree $n+1$ while the degree of $(\beta x+\gamma)f'(x)+(\delta x+\epsilon)f''(x)$ would be at most $\max\{1+(n-1), 1+(n-2)\} = n$, so it is impossible that $(x+\alpha)f(x)$ and $(\beta x+\gamma)f'(x)+(\delta x+\epsilon)f''(x)$ are equal.

5. According to Theorem 3.5, the coefficients of the associated recurrence are $\sum_{i=0}^{r} p_{i,d+i-k}(x+k)^{\underline{i}}$ for $k = 0,\dots,r+d$. As we can compute $(x+k)^{\underline{i}}$ from $(x+k)^{\underline{i-1}}$ with $\mathrm{O}(i)$ operations, the computation of a single q_k costs $\mathrm{O}(r^2)$ operations. Since we have to compute $r+d+1$ of them, the claim follows. The job can also be done with $\mathrm{O}(\mathrm{M}(r)\log(r)(r+d))$ operations in C, cf. Theorem 14.5 in [96].

6. Make an ansatz $\sum_{i=0}^{2}\sum_{j=0}^{2} p_{i,j}x^j(\frac{x^3-5x^2+5x-2}{x-1})^{(i)}$ with undetermined coefficients $p_{i,j}$, bring this expression on a common denominator and equate the coefficients of x^k in the numerator to zero. This gives a linear system for the $p_{i,j}$ which turns out to have a one-dimensional solution space. One solution corresponds to $(x-1)(79x-65)f''(x) - 4(15x^2-40x+18)f'(x) + 2(60x-119)f(x) = 0$, and all other equations of the required form are constant multiples of this one.

7. Yes. In fact, the degree of any polynomial solution must be a root of the indicial polynomial.

8. It suffices to show that p is also a solution, because the polynomial solutions form a vector space, so if p and $p+x^nq$ are solutions, then so is $2p-(p+x^nq) = p-x^nq$. The key observation is that there is a large gap in the coefficient sequence of $p+x^nq$: the coefficients of x^k for $k = \deg_x p+1,\dots,n-1$ all are zero. Since the associated recurrence of the differential equation has order at most $r+d$, which is smaller than the gap, we can replace the coefficients of x^k for $k \geq n$ by zero and obtain another solution of the recurrence. This shows that p is a solution of the differential equation.

9. True, because when f is a constant, then $f' = f'' = \cdots = f^{(r)} = 0$, so f is a solution of the equation if and only if $p_0 f = 0$, which for $f \neq 0$ is equivalent to $p_0 = 0$.

10. **a.** The indicial polynomial is $x-\alpha$, which restricts the possible values of α to the natural numbers. For every particular choice $\alpha \in \mathbb{N}$, consider an ansatz $f(x) = \sum_{k=0}^{\alpha} a_k x^k$ and define $a_{\alpha+1} = a_{\alpha+2} = 2$ for convenience. We have $f'(x) = \sum_{k=0}^{\alpha} a_k k x^{k-1}$, $f''(x) = \sum_{k=0}^{\alpha} a_k k(k-1)x^{k-2}$, so $2f''(x) - xf'(x) + \alpha f(x) = \sum_{k=0}^{\alpha}(2a_{k+2}(k+2)(k+1) - a_k k + \alpha a_k)x^k$. Since the coefficient of x^α vanishes, coefficient comparison leads to a linear system with $\alpha+1$ variables and only α equations. This must have a nontrivial solution. This shows that a nonzero polynomial solution exists if and only if $\alpha \in \mathbb{N}$; **b.** The indicial polynomial is $x-2$, so any nonzero polynomial solution must have degree two. Plug an ansatz $f(x) = a_0 + a_1x + a_2x^2$ into the equation and equate coefficients with respect to x

to obtain a linear system for a_0, a_1, a_2. This system consists of three equations, and it has a nonzero solution if and only if the determinant of the corresponding matrix vanishes. As this determinant is $-8\alpha(\alpha-3)(\alpha+3)$, we find that a polynomial solution exists if and only if $\alpha \in \{-3, 0, 3\}$; **c.** For every $\alpha \in C$, a polynomial solution is $\alpha(\alpha^2-3) + 3(\alpha-1)(\alpha+1)x + 3\alpha x^2 + x^3$.

11. Bases of the solution spaces are: **a.** $\{1, x^{-1}, x^{-2}, x^{-3}\}$; **b.** $\{\frac{x+1}{(x-1)^3(x+2)^2}\}$; **c.** $\{\frac{(x+1)(x-1)^3}{(x+2)^2}\}$; **d.** $\{\frac{1}{x}, \frac{1}{x+1}\}$; **e.** $\{\frac{1}{(1-x)^2(1+x)}\}$.

12. The solution spaces are generated by: **a.** $\{(\frac{1}{x+1}, 1, 0), (\frac{x-1}{x+1}, 0, 1)\}$; **b.** $\{(x+1, 1, 1)\}$; **c.** $\{(\frac{x^3}{(x+1)^3}, 18, -3)\}$; **d.** $\{((x+1)^2, 0, 0), (\frac{x^2(x+3)}{x+1}, 6, 0)\}$; **e.** $\{(\frac{3}{x+1}, 2, 1)\}$.

13. The algorithms of this section are applicable despite the square root in the coefficients. We first find a denominator bound $v = x + 1$. Substituting $f(x) = g(x)/(x+1)$ leads to the equation $(x+2)g''(x) + \sqrt{x}(x+2)g'(x) - \sqrt{x}g(x) = 0$ for $g(x)$, for which we get the degree bound $d = 1$. Make the ansatz $g(x) = g_0 + g_1 x$ and coefficient comparison gives a linear system for g_0, g_1 the solution space of which is generated by $(2, -1)$. The solution space is therefore generated by $\frac{x-2}{x+1}$.

14. The dimension can be any number in $\{0, 1, \ldots, r+m\}$.

15. First consider the case $\delta \neq 0$. The indicial polynomial for $\xi = -\epsilon/\delta$ is $\eta = -x(\gamma\delta - \delta^2 - \beta\epsilon + \delta^2 x)$. Since we already know that there are no polynomial solutions, the only relevant root is $1 - \frac{\gamma}{\delta} + \frac{\beta\epsilon}{\delta^2}$. Apply a change of variables $f(x) = (\delta x + \epsilon)^{1-\frac{\gamma}{\delta}+\frac{\beta\epsilon}{\delta^2}} g(x)$ with a new unknown function $g(x)$ to the equation and obtain

$$\begin{aligned}&(-\alpha\delta^2 + \beta^2\epsilon - \beta\gamma\delta + \beta\delta^2 - \delta^2 x)g(x) + \delta(\beta\delta x + 2\beta\epsilon - \gamma\delta + 2\delta^2)g'(x)\\ &+ \delta^2(\delta x + \epsilon)g''(x) = 0.\end{aligned}$$

For finding a degree bound of potential numerators, we check the indicial polynomial of this equation at infinity. Since it turns out to be $-\delta^2$, there are no candidates for numerators and hence no rational solutions when $\delta \neq 0$.

If $\delta = 0$, we must also have $\epsilon = 0$ because otherwise there are no candidate factors for the denominator of a rational solution.

If $\delta = \epsilon = 0$, we are down to a first order equation $(x+\alpha)f(x) - (\beta x + \gamma)f'(x) = 0$. We can proceed as before and determine a denominator bound for this equation under the temporary assumption $\beta \neq 0$. Doing so shows that any rational solution must have the form $f(x) = (\beta x + \gamma)^{\frac{\alpha}{\beta}-\frac{\gamma}{\beta^2}} g(x)$ for some polynomial $g(x)$. This time, we obtain $g(x) - \beta g'(x) = 0$ as the equation for the numerator, which evidently has no polynomial solutions.

If $\delta = \epsilon = \beta = 0$, we must also have $\gamma = 0$ because otherwise there are again no candidate factors for the denominator. But then we are left with a trivial equation.

16. The solution space of the differential equation in $C(x)$ is generated by $\frac{1}{1-x}$ and $\frac{x+1}{(1+2x)^2}$, so if f admits a rational closed form, it must be a C-linear combination of their expansions $\frac{1}{1-x} = 1 + x + \cdots$ and $\frac{x+1}{1+2x} = 1 - 3x + \cdots$. By solving a linear system, we find $f(x) = \frac{3}{1-x} - \frac{2(x+1)}{(1+2x)^2}$.

17. False: the solution space in $C(x)$ is generated by $\frac{1}{(1-x)(1+x)}$ and $\frac{x}{(1-x)^2(1+x)^2}$, but there is no C-linear combination of the expansions of these series which matches the first terms of f.

18. We have $f = g + q$ with $q(x) = \frac{x}{2(x+1)(x+2)}$ and $g(x) = 2 + 2x - \frac{31}{4}x^2 + \cdots$ with $4(x+1)(x+2)g''(x) + (9x^2 + 43x + 42)g'(x) + (11x + 20)g(x) = 0$.

19. **a.** True, because when ξ is an apparent singularity, the indicial polynomial at ξ has only roots in $\mathbb{N}$.

b. False. For example, $2xf'(x) - f(x) = 0$ has the indicial polynomial $2x - 1$ at zero, which has no negative integer roots, so the denominator bound does not have 0 as a root. In fact, the denominator bound is 1. However, the equation has no nonzero solution in $C[[x]]$, so 0 is not an apparent singularity.

20. Fix some r and d, plug the two desired solutions into the ansatz $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}x^j f^{(i)}(x)$, force the two resulting rational functions to zero, equate coefficients of the numerators to zero and solve the resulting linear system for the unknowns $p_{i,j}$. For the choice $r = 2$, $d = 2$, we find the equation $(x-1)^2(x+1)^2 f''(x) + 2(x-1)x(x+1)f'(x) - 4f(x) = 0$.

21. Write the differential equation as $\sum_{i=0}^{r} p_i f^{(i)} = 0$, for $p_0, \ldots, p_r \in C_{\text{sub}}[x]$, and let $b_1, \ldots, b_d$ be a basis of its solution space in $C(x)$. Since C is a C_{sub}-vector space, there are some $\alpha_1, \ldots, \alpha_m \in C$, linearly independent over C_{sub}, such that we can write $b_k = \alpha_1 b_{k,1} + \cdots + \alpha_m b_{k,m}$ for some $b_{k,\ell} \in C_{\text{sub}}(x)$. Note that we may assume m to be finite even if $\dim_{C_{\text{sub}}} C = \infty$ because the finitely many elements $b_1, \ldots, b_d$ of $C(x)$ altogether only have finitely many coefficients, and it suffices to choose for the α_ℓ's a basis of the C_{sub}-space generated by these in C.

Now observe that we have $b_k^{(i)} = \alpha_1 b_{k,1}^{(i)} + \cdots + \alpha_m b_{k,m}^{(i)}$ for every i, because the α_ℓ's are constants. Therefore, $0 = \sum_{i=0}^{r} p_i b_k^{(i)} = \sum_{\ell=0}^{m} \alpha_\ell \big(\sum_{i=0}^{r} p_i b_{k,\ell}^{(i)} \big) = 0$, which by the linear independence of the α_ℓ's implies $\sum_{i=0}^{r} p_i b_{k,\ell}^{(i)} = 0$ for all k and ℓ. Therefore, the set of all the $b_{k,\ell} \in C_{\text{sub}}$ generates the solution space of the equation in $C(x)$ as a C-vector space. The claim follows.

22. As soon as we know v, we can reduce the problem to finding rational solutions by a change of variables, so it suffices to determine which values of v can occur. Any element of $C(x^{1/v})$ admits a series expansion in $C((x^{1/v}))$, the starting indices of which are rational roots of the indicial polynomial at 0. Therefore, we cannot overlook any solutions if we take as v the least common multiple of the denominators of all the rational roots of the indicial polynomial at 0.

23. Consider a differential equation $\sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j} \exp(x)^j f^{(i)}(x) = 0$ and a solution $f(x) = \sum_{k=0}^{n} a_k \exp(x)^k$ of degree n, i.e., with $a_n \neq 0$. It suffices to deduce a bound on n from the coefficients $p_{i,j}$, because once we know a bound on n, we can determine the coefficients a_k by making an ansatz and solving a linear system.

Because of $\exp'(x) = \exp(x)$, we have $f^{(i)}(x) = \sum_{k=0}^{n} a_k k^i \exp(x)^k$ for every i. Therefore,

$$\sum_{i=0}^{r} \sum_{j=0}^{d} \sum_{k=0}^{n} p_{i,j} a_k k^i \exp(x)^{k+j} = 0,$$

and taking the coefficient of $\exp(x)^{n+d}$ gives in particular $\sum_{i=0}^{r} p_{i,d} a_n n^i = 0$. Since $a_n \neq 0$ and d can be chosen such that $p_{i,d} \neq 0$ for at least one i (otherwise the equation is just $0 = 0$), this is a nonzero polynomial equation for n. As such, it can only have finitely many integer roots, the largest of which can serve as degree bound.

24. Setting $g = f^2$, we can use closure properties to find the equation

$$\begin{aligned}(x+1)(x-1)^2 g'''(x) - 3(x^2-2x-2)(x-1)g''(x) + 2(x^3-3x^2+5)g'(x)\\ - 2(2x-5)(x-1)g(x) = 0,\end{aligned}$$

whose solution space in $C(x)$ is generated by $(x-2)(x+1)/(x-1)$. Therefore, if the original equation has solutions of the requested form, they can only be $\sqrt{c(x-2)(x+1)/(x-1)}$ for some constant c. Plugging this expression into the given equation and simplifying confirms that they are indeed solutions.

25. We have $\deg_y H = r$ and $H = \eta p$ for some polynomial $p \in C[x, y]$. Because of the assumed irreducible factor, $\deg_y p > 0$, so $\deg_y \eta < r$. The claim follows.

26. Yes, but the resulting indicial polynomials are in general not useful for predicting denominators. For example, for the equation $x(1-x)f'(x) - (1-3x)f(x) = 0$ and $v = x(1-x)$, we would get the indicial polynomial $\eta = 1$, so we might overlook the rational solution $\frac{1}{x(1-x)^2}$.

27. For example, for the differential equation $(x^2-2)f'(x) - f(x) = 0$ the indicial polynomial with respect to $v = x^2 - 2$ turns out to be 1, i.e., it is only a polynomial of degree zero while the equation has order one. At the same time, $\sqrt{2}$ and $-\sqrt{2}$ are regular singularities of the equation.

Section 3.6

1. This follows directly from Theorem 3.25.

2. This follows directly from Theorem 3.29.

3. False: $h(x) = x + 1$ is hyperexponential but $h(\sqrt{x}) = 1 + \sqrt{x}$ is not.

4. If h satisfies the equation $vh' - uh = 0$ for some u, v, then h^q satisfies the equation $v(h^q)' - uq(h^q) = 0$.

5. **a.** True. "$\Leftarrow$": $f'(x)/f(x) = g'(x)$ is a derivative. "$\Rightarrow$": $\frac{f'(x)}{f(x)} = g'(x) + \sum_{i=1}^m \alpha_i \frac{h_i'(x)}{h_i(x)}$ is a derivative if and only if $\sum_{i=1}^m \alpha_i \frac{h_i'(x)}{h_i(x)}$ is a derivative. Since the h_i are assumed to be squarefree and pairwise coprime, this forces $\alpha_1 = \cdots = \alpha_m = 0$. See Theorem 5.2 for a more detailed argument. **b.** "$\Rightarrow$" is False: For example, $\exp(1/x)x$ is a kernel. "$\Leftarrow$" is True: Let $u, v \in C[x]$ be coprime such that $\frac{f'}{f} = \frac{u}{v}$. We show that the existence of an integer β with $\gcd(u - \beta v', v) \neq 1$ implies that at least one of the α_i is an integer. Consider an irreducible factor w of $\gcd(u - \beta v', v)$. Then w is a factor of v with multiplicity one, because if the multiplicity was higher, then $w \mid v'$ would imply $w \mid u$ in contradiction to u and v being coprime. Thus, if we write $\frac{u}{v} = g' + \sum_{i=1}^m \alpha_i \frac{h_i'}{h_i}$, then w cannot appear in the denominator of g', so we must have $w \mid h_i$ for some i. Since $h_1, \ldots, h_m$ are assumed to be pairwise coprime, this i is uniquely determined, and we may assume without loss of generality that $h_i = w$. (Otherwise, if $h_i = w\tilde{h}_i$, for some $\tilde{h}_i$, use $\frac{h_i'}{h_i} = \frac{w'}{w} + \frac{\tilde{h}_i'}{\tilde{h}_i}$ to separate the portion of interest from the rest.) We may also assume that $i = 1$. Let $\tilde{v}$ be such that $v = w\tilde{v}$. Then $w \mid u - \beta v' = vg' + \alpha_1 v \frac{w'}{w} + v \sum_{i>1} \alpha_i \frac{h_i'}{h_i} - \beta(w'\tilde{v} + w\tilde{v}')$ implies $w \mid (\alpha_1 - \beta)\tilde{v}w'$. Since w is not contained in $\tilde{v}$ nor in w', this implies $\alpha_1 = \beta$.

6. "$\Rightarrow$": Let $q_1, q_2 \in K$ be such that $D(y_i)/y_i = q_i$ for $i = 1, 2$. If $y_1 + y_2$ is hyperexponential, then

$$\frac{D(y_1 + y_2)}{y_1 + y_2} = \frac{q_1 y_1 + q_2 y_2}{y_1 + y_2} =: q \in K$$

implies $q_1 y_1 + q_2 y_2 = q y_1 + q y_2$, so $(q_1 - q)y_1 = (q - q_2)y_2$.

Case 1: $q_1 = q$. Then, because hyperexponential functions are not zero, also $q = q_2$, so $q_1 = q_2$, which implies $D(y_1/y_2) = 0$, so $y_1/y_2 \in \mathrm{Const}(E) = \mathrm{Const}(K) \subseteq K$.

Case 2: $q_1 \neq q$. Then $y_1/y_2 = (q - q_2)/(q_1 - q) \in K$.

"$\Leftarrow$": If $y_1/y_2 = q \in K$, then $y_1 + y_2 = (1 + q)y_2$, which is obviously hyperexponential.

7. Let $q \in K$ and $m_0, \ldots, m_{d-1} \in K$ be such that $D(y) = qy$ and $m_0 + m_1 y + \cdots + m_{d-1} y^{d-1} + y^d = 0$. We may assume that d is chosen minimally. Differentiating the minimal polynomial gives

$$\begin{aligned}
0 &= D(m_0) + D(m_1)y + \cdots + D(m_{d-1})y^{d-1} + D(1) \\
&\quad + 0 + m_1 qy + \cdots + m_{d-1}(d-1)y^{d-2}qy + dy^{d-1}qy \\
&= D(m_0) + (D(m_1) + m_1 q)y + \cdots + (D(m_{d-1}) + (d-1)m_{d-1}q)y^{d-1} + dqy^d
\end{aligned}$$

$$= (D(m_0) - dm_0q) + (D(m_1) - (d-1)m_1q)y + \cdots$$
$$+ (D(m_{d-1}) - m_{d-1}q)y^{d-1}.$$

By the minimality of d, it follows that $D(m_i) = (d-i)m_iq$ for $i = 0, \ldots, d-1$. By the minimality of d, it also follows that $m_0 \neq 0$. Since $D(y^d) = dy^{d-1}D(y) = dqy^d$, we find that $y^d/m_0 \in \mathrm{Const}(E) = \mathrm{Const}(K)$. The claim follows.

8. "$\Rightarrow$": Suppose that $\mathrm{Const}(E) = \mathrm{Const}(K)$. By the previous exercise, the equation $D(y) = qy$ can only have an algebraic solution if there is some $d \in \mathbb{N}$ for which the equation $D(y) = dqy$ has a nonzero solution in K. If this is the case and $r \in K$ is such a solution, then $D(r/h^d) = \frac{D(r)h^d - rD(h^d)}{h^{2d}} = 0$ implies that $r/h^d \in \mathrm{Const}(E)$, which is a contradiction since $\mathrm{Const}(E) = \mathrm{Const}(K)$ and $r/h^d \notin \mathrm{Const}(K) \subseteq K$, because h is transcendental.

"$\Leftarrow$": Suppose that $\mathrm{Const}(K) \subsetneq \mathrm{Const}(E)$. We show that the equation $D(y) = qy$ has a solution in an algebraic extension of K. Let $r = \frac{u}{v} \in K(x) \setminus K$ be such that $r(h)$ is a constant. Then $D(u(h))/u(h) = D(v(h))/v(h)$. Since we may assume that u and v are coprime, we must have $u(h) \mid D(u(h))$ and $v(h) \mid D(v(h))$ in $K[h]$. Writing $u = u_0 + u_1x + \cdots + u_nx^n$, we have $D(u(h)) = \sum_{i=0}^n (D(u_i) + iqu_i)h^i$, so $u(h) \mid D(u(h))$ implies that there exists a $c \in K$ such that $D(u_i) + iqu_i = cu_i$ for $i = 0, \ldots, n$. If u has at least two nonzero terms, say $u_i, u_j \neq 0$ for some $i \neq j$, then it follows that $D(u_i)u_j + iqu_iu_j = D(u_j)u_i + jqu_iu_j$, which leads to $D(u_i/u_j) = (j-i)qu_i/u_j$, so in this case, $(u_i/u_j)^{1/j-i}$ is a nonzero algebraic solution of $D(y) = qy$. Similarly, we can construct a nonzero algebraic solution if v has at least two nonzero terms. There remains the case where both u and v have only one nonzero term. In this case, we must have $r = ch^k$ for some $c \in \mathbb{K} \setminus \{0\}$ and some $k \in \mathbb{Z}$. In this case, $D(r) = 0$ implies $D(c) = -ckq$, so $c^{-1/k}$ is an algebraic solution.

9. If P is the differential operator with $P \cdot (h_1 + h_2) = 0$, then, since P is linear, $(P \cdot h_1) + (P \cdot h_2) = 0$, or $P \cdot h_1 = -P \cdot h_2$. Now if $P \cdot h_1$ and $P \cdot h_2$ were not zero, they would be hyperexponential terms similar to h_1 and h_2, respectively, and since h_1, h_2 are not similar to each other by assumption, also $P \cdot h_1$ and $P \cdot h_2$ would not be similar to each other, although they are equal. Since this is impossible, we must have $P \cdot h_1 = P \cdot h_2 = 0$.

10. The equation $(x+1)f'(x) - f(x) = 0$ has the solution $x+1$, but neither x nor 1 is a solution.

11. False: $\exp(x)\sqrt{x}$ is neither exponential nor algebraic.

12. True. If g is a rational function, then g' has no simple poles, and when $y = p/q$ is a rational function, then $y'/y = (p'q - pq')/(pq) = p'/p - q'/q$ has no multiple poles. So the only remaining chance for having $y'/y = g'$ is when g is a polynomial. But $p'/p - q'/q$ cannot be a polynomial of positive degree, because the denominator degrees are larger than the numerator degrees. It remains that g is constant, so $g' = 0$, so $y'/y = 0$, so $y' = 0$, so y is constant. The converse is obvious.

13. **a.** $\frac{x+3}{x+1}e^x$; **b.** $\frac{x+\alpha}{x+1}e^x$ for any $\alpha \in C$.

14. **a.** no way; **b.** $\frac{(55x^2-70x+47)e^{x-x^2}}{\sqrt{x+1}}$.

15. "$\Rightarrow$": If y_1, y_2 are similar then y_1/y_2 is a rational function, so if $y_2 = ks$ is a decomposition of y_2 into a kernel and a shell, then $y_1 = k(sy_1/y_2)$ is a decomposition of y_1 into a kernel and shell, with the same kernel.

"$\Leftarrow$": If y_1, y_2 have the same set of kernels, then we have $y_1 = ks_1$ and $y_2 = ks_2$ for some kernel k and some rational functions s_1, s_2. It follows that $y_1/y_2 = s_1/s_2$ is rational, so y_1, y_2 are similar.

16. The kernels are $\exp((x+1)^2/x)x^a(x+2)^{b+1/2}(x+3)^{c-1/5}$ for arbitrary $a, b, c \in \mathbb{Z}$, with $x^{-a}(x+2)^{-b}(x+3)^{-c}(x+4)$ being the corresponding shells.

17. Multiply the equation by $h(x) = \exp(\int q(x))$ and observe that $h'(x) = h(x)q(x)$ and $h''(x) = h(x)(q(x)^2 + q'(x))$. Searching for a rational solution of the nonlinear equation is therefore equivalent to searching for a hyperexponential solution of the equation $h''(x) = \frac{2}{3(x+1)^2}h(x) - \frac{4x+1}{3(x+1)^2}h'(x)$. A solution is $h(x) = \exp(-\frac{1}{x+1})(x+1)^{2/3}$, which corresponds to $q(x) = \frac{2x+3}{3(x+1)^2}$. Nonlinear equations which can be translated to linear equations like in this example are called *Riccati equations.*

18. For example $y_1 y_2^5 y_3 - x^6$ or $y_2^9 y_3^3 - x^5$.

19. **a.** $e^{(-1+\sqrt{3})x}/(x+1)$ and $e^{(-1+\sqrt{3})x}/(x+1)$; **b.** none; **c.** $e^{2x^2}(1-x)^2$; **d.** $(\alpha x^3 + \beta x^{-1})e^{2x^2-3x+1/x}$ for any constants α, β; **e.** $e^{-x}(3x+1)$ and $(3x+1)^2$.

20. The only choice is $\alpha = 1$, for which there is the solution $\frac{x}{x+1}e^x$.

21. $81(4x+9)(x+1)^2 f''(x) - 9(4x-1)(10x+27)(x+1)f'(x) + (36x^3 - 167x^2 - 1247x - 1089)f(x) = 0$. One way to find this equation is by applying guessing to a series expansion of a linear combination of the two required solutions.

22. Yes. Write $H = H_1 \cup H_2 \cup \cdots \cup H_k$, where each H_i $(i = 1, \ldots, k)$ is one of the sets added to H in line 8. Since we choose bases in line 7, each H_i is linearly independent. Furthermore, all elements of a set H_i are similar to each other. On the other hand, elements from two distinct sets H_i, H_j $(i \neq j)$ are not similar because at least at one singularity they have different types. Any linear combination of elements of H is a linear combination of certain linear combinations of elements of the linearly independent sets H_i. Therefore, if H were linearly dependent, there would be some hyperexponential function which could be written as a linear combination of certain other hyperexponential functions that are not similar to it. According to Exericse 6, this is not possible.

23. False. Consider an equation whose only hyperexponential solution is a certain function h. We can write $h = \frac{h}{x}x = \frac{h}{x}\int 1 = \frac{h}{x}\int \frac{v_1 h/x}{v_1 h/x} = h_1 \int \frac{h_2}{v_1 h_1}$ with $h_1 = h/x$ and $h_2 = v_1 h/x$. Since h is supposed to be the only hyperexponential solution, h_1 is not a solution although $h_1 \int \frac{h_2}{v_1 h_1}$ is.

24. False. Example 3.76 has a counterexample.

25. $P \cdot f = 0$ means $(u - vD)L \cdot f = 0$, which means $(u - vD) \cdot (L \cdot f) = 0$. Since f is not supposed to be a solution of L, we have $L \cdot f \neq 0$. Since $u - vD$ is a first order operator, all its solutions are constant multiples of h, so $L \cdot f = ch$ for some $c \neq 0$. This equation has a solution f iff the equation with $c = 1$ has a solution.

26. One is the hyperexponential function h with $uh - vh' = 0$ and the second is the d'Alembertian solution $h \int \frac{1}{v}$, which cannot be a constant multiple of h.

27. This is classic: consider the factorization $c_0 + c_1 x + \cdots + c_r x^r = c_r \prod_{i=1}^{k} (x - \xi_i)^{e_i}$ for pairwise distinct $\xi_i \in C$. Then the solutions of the equation are the hyperexponential functions $x^j \exp(\xi_i x)$ for $i = 1, \ldots, k$ and $j = 0, \ldots, e_i - 1$.

28. By definition of the a_i, we have $(v_{i-1}D - u_{i-1}) \cdot a_i = a_{i-1}$ for all $i > 0$. This implies the claim in the hint. It is also clear from the definition of the a_i that $(v_{i-1}D - u_{i-1}) \cdots (v_1 D - u_1) \cdot a_j = 0$ for all $j < i$. Therefore, applying $(v_{i-1}D - u_{i-1}) \cdots (v_1 D - u_1)$ to any linear combination $\alpha_1 a_1 + \cdots + \alpha_i a_i$ with $\alpha_1, \ldots, \alpha_i \in C$ yields $\alpha_i h_i$. If $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ are such that $\alpha_1 a_1 + \cdots + \alpha_m a_m = 0$, then $\alpha_1 = \cdots = \alpha_m = 0$, because if not all of them are zero, let i be maximal with $\alpha_i \neq 0$ and apply $(v_{i-1}D - u_{i-1}) \cdots (v_1 D - u_1)$ to obtain $\alpha_i h_i = 0$, which forces $\alpha_i = 0$.

Section 4.1

1. It is clear that $\delta(p + q) = \delta(p) + \delta(q)$ for all $p, q \in C[x]$. We also have $\delta(pq) = p(x + 1)q(x + 1) - p(x)q(x) = p(x + 1)q(x + 1) - p(x + 1)q(x) + p(x + 1)q(x) - p(x)q(x) = \sigma(p)\delta(q) + \delta(p)q$ for all $p, q \in C[x]$, as required.

2. **a.** $x\partial^4 + (x^2 + 1)\partial^2 - 2x\partial + x$ and $(x^2 - 1)\partial^2 + (-3x^2 + x + 2)\partial - 6x$; **b.** $(x+2)\partial^4 - 2\partial^3 + (x^2+1)\partial^2 - 2x\partial + x$ and $(x^2+2x+1)\partial^2 + (-3x^2 - 7x - 4)\partial + 1$; **c.** $x^4\partial^4 + (10x^4 - 10x^2 - 2)\partial^3 + (25x^4 - 49x^2 + 25x + 1)\partial^2 - 2x\partial + x$ and $(x^5 + x^4 - x - 1)\partial^2 + (10x^5 + 7x^4 - 10x^3 - 11x^2)\partial + 25x^5 + 10x^4 - 50x^3 - 15x^2 + 30x + 1$.

3. Induction on n. For $n = 0$ there is nothing to show. Suppose it is true for some $n \in \mathbb{N}$. Then

$$D^{n+1}x^k = D(D^n x^k) = \sum_i \binom{n}{i} k^{\underline{i}} D x^{k-i} D^{n-i}$$

$$= \sum_i \binom{n}{i} k^{\underline{i}} (x^{k-i} D + (k - i)x^{k-i-1}) D^{n-i}$$

$$= \sum_i \binom{n}{i} k^{\underline{i}} x^{k-i} D^{n-i+1} + \underbrace{\sum_i \binom{n}{i} k^{\underline{i+1}} x^{k-(i+1)} D^{n-i}}_{=\sum_i \binom{n}{i-1} k^{\underline{i}} x^{k-i} D^{n-(i+1)}}$$

$$= \sum_i (\underbrace{\binom{n}{i} + \binom{n}{i-1}}_{=\binom{n+1}{i}}) k^{\underline{i}} x^{k-i} D^{(n+1)-i}.$$

4. For $m = 0$ the claim reduces to $\delta(1) = 0$, which is always true. Suppose it holds for some $m \in \mathbb{N}$. Then

$$\begin{aligned} \delta(\overline{\sigma^{m+1}}(p)) &= \delta(p\overline{\sigma^m}(\sigma(p))) = \delta(p)\overline{\sigma^m}(\sigma(p)) + \sigma(p)\delta(\overline{\sigma^m}(\sigma(p))) \\ &= \delta(p)\overline{\sigma^m}(\sigma(p)) + \sigma(p)\delta(\sigma(p) + \cdots + \sigma^m(p))\overline{\sigma^{m-1}}(\sigma^2(p)) \\ &= \delta(p + \sigma(p) + \cdots + \sigma^m(p))\overline{\sigma^m}(\sigma(p)), \end{aligned}$$

as claimed.

5. For $p, q \in R$ with $q \neq 0$, we must have $\bar\sigma(\frac{p}{q}) = \frac{\bar\sigma(p)}{\bar\sigma(q)} = \frac{\sigma(p)}{\sigma(q)}$. Any σ-derivation δ must satisfy $\delta(1) = 0$, because $\delta(1) = \delta(1 \cdot 1) = \delta(1)1 + \sigma(1)\delta(1) = 2\delta(1)$. Therefore, $0 = \delta(1) = \bar\delta(1) = \bar\delta(\frac{q}{q}) = \bar\delta(q)\frac{1}{q} + \bar\sigma(q)\bar\delta(\frac{1}{q})$ and hence $\bar\delta(\frac{1}{q}) = -\frac{\bar\delta(q)}{q\bar\sigma(q)} = -\frac{\delta(q)}{q\sigma(q)}$, and in general $\bar\delta(\frac{p}{q}) = \bar\delta(p)\frac{1}{q} + \bar\sigma(p)\bar\delta(\frac{1}{q}) = \frac{\delta(p)\sigma(q) - p\delta(q)}{q\sigma(q)}$.

6. $p = \partial^{-1}\partial p = \partial^{-1}\sigma(p)\partial + \partial^{-1}\delta(p)$. Now multiply by ∂^{-1} from the right.

7. **a.** False. Counterexample: $L = D \in C(x)[D]$, $m = 1 \in C(x)$, $y = x \in C(x)$. **b.** False. Counterexample: $L = xD \in C(x)[D]$, $m = 1 \in C(x)$, $y = x \in C(x)$.

8. For any $p, q \in K$ we have $\delta(pq) = \delta(qp)$, which implies $\delta(p)q + \sigma(p)\delta(q) = \delta(p)p + \sigma(q)\delta(p)$, or $\delta(q)(\sigma(p) - p) = \delta(p)(\sigma(q) - q)$. **a.** Let $p \in K$ be such that $\sigma(p) \neq p$ and define $u = \delta(p)/(\sigma(p) - p)$. Then for every $q \in K$ the relation above implies $\delta(q) = \frac{\delta(p)}{\sigma(p)-p}(\sigma(q) - q) = u(\sigma(q) - q)$, as claimed. **b.** Let $p \in K$ be such that $\delta(p) \neq 0$ and define $u = (\sigma(p) - p)/\delta(p)$. Then for every $q \in K$, the relation above implies $\sigma(q) = \delta(q)(\sigma(p) - p)/\delta(p) + q = u\delta(q) + q$, as claimed.

9. Not true in general. For a counter example, take $\sigma, \delta\colon C[x] \to C[x]$, $\sigma(p(x + 1)) = p(x)$ and $\delta(p(x)) = x^2(p(x + 1) - p(x))$. Then σ is an endomorphism, δ is a σ-derivation, but $\sigma(\delta(x)) = \sigma(x^2(x + 1 - x)) = (x + 1)^2$ while $\delta(\sigma(x)) = x^2(x + 1 - 1) = x^2$.

10. **a.** True. If $p \in \mathrm{Const}(R)$, then $\sigma(p) = p$ and $\delta(p) = 0$. Consequently, we have $\partial p = \sigma(p)\partial + \delta(p) = p\partial$ and therefore $pq = qp$ for every $q = q_0 + q_1\partial + \cdots + q_r\partial^r \in R[\partial]$. **b.** False. Take $R = \mathbb{C}$, σ as conjugation, $\delta = 0$. Then $\mathrm{Const}(R) = \mathbb{R}$ but since $\sigma^2 = \mathrm{id}$, we have $\partial^2 q = q\partial^2$ for all $q \in R[\partial]$.

11. **a.** $D + \frac{2}{x^2-1}$; **b.** $S - \frac{x^2+x-2}{x^2+x}$; **c.** $M_2 - \frac{1+x^2}{(1+x)^2}$.

12. Yes, it is an Ore algebra. We have $\sigma = \mathrm{id}$ and $\delta = 0$. But no, $C((x))$ does not become a $C(x)[Y]$-module with the proposed action, because $Y^2 \cdot f = f^2$ is inconsistent with $Y^2 \cdot f = Y \cdot (Y \cdot f) = Y \cdot f = f$.

13. Let $P = p_0 + p_1 M_2 + \cdots + p_r M_2^r \in C(x)[M_2]$ be an annihilating operator of $\exp(x)$. We have to show that $P = 0$. If it is not, then we may assume that $p_r = 1$ and that r is minimal. Then $P \cdot \exp(x) = 0$ implies $\sum_{i=0}^r p_i(x)\exp(x^{2^i}) = 0$. Differentiating with respect to x gives $\sum_{i=0}^r p_i'(x)\exp(x^{2^i}) + p_i(x)x^{2_i-1}\exp(x^{2^i}) = 0$, and eliminating the term $\exp(x^{2^r})$ from the two equations gives $\sum_{i=0}^{r-1}(p_i'(x) - p_i(x)(x^{2^r-1} - x^{2^i-1}))\exp(x^{2^i}) = 0$. By minimality of r, each rational function p_i must satisfy the differential equation $p_i'(x) = (x^{2^r-1} - x^{2^i-1})p_i(x)$, and since there are no nonzero solutions, we have $p_0 = \cdots = p_{r-1} = 0$. But this would imply that $P \cdot \exp(x) = \exp(x^{2^r}) = 0$, and since this is not the case, no nonzero P can exist and the claim follows.

It can be shown more generally that whenever $y \in C((x))$ is D-finite with respect to a Mahler operator and with respect to D_x, then y is rational [64, Theorem 1–3].

14. A q-shift-recurrence is $xq^2 f(q^3x) - xqf(q^2x) - f(qx) + f(x) = 0$. If $f(x)$ were D-finite with respect to D, its coefficient sequence $(q^{n^2})_{n=0}^{\infty}$ would be D-finite with respect to S, but this is not the case. For, if we had $\sum_{i=0}^r \sum_{j=0}^d p_{i,j} n^j q^{(n+i)^2} = 0$, then $\sum_{i=0}^r \sum_{j=0}^d q^{i^2} p_{i,j} n^j (q^{2i})^n = 0$, and by the linear independence of pairwise distinct exponential sequences over the rational function field, it follows that $p_{i,j} = 0$ for all i and j.

15. False. Counterexample: $L = D$ and $M = D + x$. Then $LM = D^2 + xD + 1$, and for every $\tilde{M} \in C(x)[\partial]$ we have $[D^0](\tilde{M}L) = 0 \neq 1 = [D^0](LM)$.

16. If $p_0 + p_1 S + \cdots + p_r S^r \in C[x][S]$ is a nonzero annihilating operator of $(a_n)_{n=0}^{\infty}$, then so is $p_0 + p_1(\Delta + 1) + \cdots + p_r(\Delta + 1)^r \in C[x][\Delta]$, and if $q_0 + q_1\Delta + \cdots + q_r S^r \in C[x][\Delta]$ is a nonzero annihilating operator of $(a_n)_{n=0}^{\infty}$, then so is $q_0 + q_1(S - 1) + \cdots + q_r(S - 1)^r \in C[x][\Delta]$.

17. It follows from the commutation rule that we always have $\mathrm{ord}(LM) \leq \mathrm{ord}(L) + \mathrm{ord}(M)$ and that $[\partial^{\mathrm{ord}(L)+\mathrm{ord}(M)}](LM) = \mathrm{lc}(L)\sigma^{\mathrm{ord}(L)}(\mathrm{lc}(M))$, so the only question is whether or not this coefficient can be zero.

"$\Leftarrow$": If R is an integral domain and σ is injective, then it is clear that $\mathrm{lc}(L)\sigma^{\mathrm{ord}(L)}(\mathrm{lc}(M))$ is nonzero for any choice of $L, M \in R[\partial] \setminus \{0\}$. "$\Rightarrow$": If the coefficient cannot be zero, then in particular for any $p, q \in R \setminus \{0\}$ we have $pq \neq 0$ (taking $L = q$, $M = q$) and for any $p \in R$ we have $\sigma(p) \neq 0$ (taking $L = \partial$ and $M = p$), so R is an integral domain and σ is injective.

18. For fixed constants $u, v \neq 0$, consider $f = 1/(1 - ux)$ and $g = 1/(1 - vx)$. Then $m(f, g) = 1/(1 - uvx)$, $m(f, g)' = uv/(1 - uvx)^2$, $m(f', g) = u/(1 - uvx)^2$, $m(f, g') = v/(1 - uvx)^2$, $m(f', g') = uv(1 + uvx)/(1 - uvx)^3$. Now make an ansatz

$$\frac{uv}{(1-uvx)^2} = \alpha\frac{1}{1-uvx} + \beta\frac{u+v}{(1-uvx)^2} + \gamma\frac{uv(1+uvx)}{(1-uvx)^3},$$

clear denominators, and compare coefficients with respect to u, v, and x in order to find $\alpha, \beta, \gamma \in C$ that hold for all choices of u, v. The resulting inhomogeneous linear system for α, β, γ turns out to have no solution.

19. From $\partial \cdot \tilde{m}(f, g) = \partial \cdot qm(f, g) = \partial q \cdot m(f, g) = (\sigma(q)\partial + \delta(q)) \cdot m(f, g)$, it follows that we must have $\tilde{\alpha} = (\sigma(q)\alpha + \delta(q))/q$, $\tilde{\beta} = \sigma(q)\beta/q$, $\tilde{\gamma} = \sigma(q)\gamma/q$.

20. We need $(\partial p) \cdot (a \otimes b) = (\sigma(p)\partial + \delta(p)) \cdot (a \otimes b)$ for all a, b. In particular,

$$\begin{aligned}
(\partial p) \cdot (1 \otimes 1) &= \partial \cdot (p \otimes 1) = \alpha(p \otimes 1) + \beta(\partial p \otimes 1) + \beta(p \otimes \partial) + \gamma(\partial p \otimes \partial)\\
&= \alpha(p \otimes 1) + \beta((\sigma(p)\partial + \delta(p) \otimes 1) + \beta(p \otimes \partial) + \gamma((\sigma(p)\partial + \delta(p)) \otimes \partial)\\
&= (\alpha p + \beta\delta(p))(1 \otimes 1) + (\beta p + \gamma\delta(p))(1 \otimes \partial) + \beta\sigma(p)(\partial \otimes 1) + \gamma\sigma(p)(\partial\otimes\partial)
\end{aligned}$$

and

$$\begin{aligned}
(\sigma(p)\partial + \delta(p)) \cdot (1 \otimes 1) = \sigma(p)(\alpha(1 \otimes 1) + \beta(\partial \otimes 1)&\\
+ \beta(1 \otimes \partial) + \gamma(\partial \otimes \partial) + \delta(p)(1 \otimes 1).&
\end{aligned}$$

Since the elements $(1 \otimes 1)$, $(1 \otimes \partial)$, $(\partial \otimes 1)$, $(\partial \otimes \partial)$ of $(K[\partial]/\langle L\rangle) \otimes (K[\partial]/\langle M\rangle)$ are linearly independent when $\operatorname{ord}(L), \operatorname{ord}(M) > 1$, we can equate coefficients and obtain the claimed relations.

21. For all $P \in K[\partial]$ we have $P \cdot ([1], [1]) = ([P], [P])$, and the latter is equal to $([0], [0])$ in $(K[\partial]/\langle L\rangle) \times (K[\partial]/\langle M\rangle)$ if and only if $P \in \langle L\rangle$ and $P \in \langle M\rangle$. The first claim follows. For the second claim, note that $\langle L\rangle \cap \langle L\rangle = \langle L\rangle$, and that $\langle L\rangle$ contains L but no operator of order smaller than $\operatorname{ord}(L)$.

22. This follows directly from the natural identifications of $(V_1 \times V_2) \times V_3$ with $V_1 \times (V_2 \times V_3)$ and $(V_1 \otimes V_2) \otimes V_3$ with $V_1 \otimes (V_2 \otimes V_3)$, which apply to any three K-vector spaces V_1, V_2, V_3.

23. This follows directly from the natural identification of $V \otimes (W_1 \times W_2)$ with $(V \otimes W_1) \times (V \otimes W_2)$, which applies to any three K-vector spaces V, W_1, W_2.

24. Let $k \geq 2$ be an integer. Since $(a_n(q))_{n=0}^{\infty}$ is D-finite, there is a nonzero annihilating operator $L \in C(q)(x)[Q]$, say of order r. Since we may multiply from the left with a rational function, we may assume that L has coefficients in $C(q)[x]$, say of degree at most d. For any other operator $M \in C(q)[x][Q]$, the product $ML \in C(q)[x][Q]$ is a nonzero annihilating operator of $(a_n(q))_{n=0}^{\infty}$. Make an ansatz $M = \sum_{i=0}^{u}\sum_{j=0}^{ku-d} m_{i,j}x^i Q^j$ with undetermined $u \in \mathbb{N}$ and undetermined coefficients $m_{i,j} \in C(q)$ and consider the product ML. Its coefficients with respect to x and Q will be $C(q)$-linear combinations of the undetermined coefficients. Equating all coefficients of powers of x that are not divisible by k to zero gives a linear system of $(u+r+1)(u-d+1) = u^2+\mathrm{O}(u)$ equations and $(u+1)(ku-d+1) = ku^2 + \mathrm{O}(u)$ variables. Since $k \geq 2$, the system will have more variables than equations when u is chosen sufficiently large. For such a u, the system will have a nontrivial solution, and the corresponding operator ML is an annihilating operator for $(a_n(q))_{n=0}^{\infty}$ with the property stated in the hint.

Write this operator as $P = \sum_{i,j} p_{i,j} x^{kj} Q^j \in C(q)[x][Q]$, so that $\sum_{i,j} p_{i,j} q^{nkj} a_{n+i}(q) = 0$ for all $n \in \mathbb{N}$. Replacing q by ωq some $\omega \in C$ gives $\sum_{i,j} p_{i,j} \omega^{nkj} q^{nkj} a_{n+i}(\omega q) = 0$. If ω is a kth root of unity, then $\omega^{knj} = 1$, so P is an annihilating operator for $(a_n(\omega q))_{n=0}^{\infty}$ in this case. This completes the proof. This example is taken from [202].

25. We have $(M_2^4 + (x^8 + x^7 - x^6)M_2^2 + x^9) \cdot (f + g) = 0$ and $(M_2^3 + (-x^5 + x^4)M_2^2 + (-x^8 + x^7)M_2 + x^9) \cdot (fg) = 0$. For the latter, note that that we need to choose $\alpha = 0, \beta = 0, \gamma = 1$.

26. **a.** True by Theorem 4.12, Part 2. **b.** True: If $M \in K[\partial] \setminus \{0\}$ is such that $M \cdot g = 0$, then $(ML) \cdot f = 0$, and since ML is not zero when L and M are not zero, f is D-finite.

27. Let $f_1, f_2 \in F$ be such that $L \cdot f_1 = L \cdot f_2 = 0$. By assumption, $M \cdot m(f_1, f_1) = M \cdot m(f_2, f_2) = M \cdot m(f_1 + f_2, f_1 + f_2) = 0$. Since m is bilinear, we have $m(f_1 + f_2, f_1 + f_2) = m(f_1, f_1) + m(f_1, f_2) + m(f_2, f_1) + m(f_2, f_2) = m(f_1, f_1) + 2m(f_1, f_2) + m(f_2, f_2)$, so $0 = M \cdot m(f_1 + f_2, f_1 + f_2) = M \cdot m(f_1, f_1) + 2M \cdot m(f_1, f_2) + M \cdot m(f_2, f_2) = 2M \cdot m(f_1, f_2)$.

Section 4.2

1. **a.** True. If P, Q are such that $A = PC + \mathrm{rrem}(A, C)$ and $B = QC + \mathrm{rrem}(B, C)$ then $A + B = (P + Q)C + \mathrm{rrem}(A, C) + \mathrm{rrem}(B, C)$, and since $\mathrm{ord}(\mathrm{rrem}(A, C)), \mathrm{ord}(\mathrm{rrem}(B, C)) < \mathrm{ord}(C)$ implies $\mathrm{ord}(\mathrm{rrem}(A, C) + \mathrm{rrem}(B, C)) < \mathrm{ord}(C)$, the uniqueness of the right remainder implies that $\mathrm{rrem}(A+B, C) = \mathrm{rrem}(A, C)+\mathrm{rrem}(B, C)$. **b.** True. We have $B = \mathrm{rquo}(B, C)C+ \mathrm{rrem}(B, C)$, so

$$\begin{aligned}&\mathrm{rrem}(AB, C) = \mathrm{rrem}(A\mathrm{rrem}(B, C) + A\mathrm{rquo}(B, C)C, C)\\ &= \mathrm{rrem}(A\mathrm{rrem}(B, C), C) + \mathrm{rrem}(A\mathrm{rquo}(B, C)C, C) = \mathrm{rrem}(A\mathrm{rrem}(B, C), C),\end{aligned}$$

where we have used part a in step 2. **c.** False. For $A = D^2 - x$, $B = D^2 - 1$, and $C = D + x \in \mathbb{Q}(x)[D]$ we have $\mathrm{rrem}(\mathrm{rrem}(A, C)B, C) = x^4 - x^3 - 3x^2 + 2x + 2$ and $\mathrm{rrem}(AB, C) = x^4 - x^3 - 7x^2 + 2x + 4$.

2. If $G, G' \in K[\partial]$ are two greatest common right divisors of U and V, then G must be a left multiple of G' and vice versa. This implies $\operatorname{ord}(G) = \operatorname{ord}(G')$, so we have $G = cG'$ for some $c \in K$. Because of $\operatorname{lc}(G) = \operatorname{lc}(G') = 1$, we must have $c = 1$, which shows that $G = G'$.

If $L, L' \in K[\partial]$ are two least common left multiples of U and V, then L must be a right divisor of L' and vice versa. This implies $\operatorname{ord}(L) = \operatorname{ord}(L')$, so we have $L = cL'$ for some $c \in K$. Because of $\operatorname{lc}(L) = \operatorname{lc}(L') = 1$, we must have $c = 1$, which shows that $L = L'$.

3. For all $P \in K[\partial]$, we have: P is a common right divisor of U and $\operatorname{gcrd}(V, W)$ if and only if P is a common right divisor of U, V, W if and only if P is a common right divisor of $\operatorname{gcrd}(U, V)$ and W. Since left hand side and right hand side have the same right divisors, they are in particular right divisors of each other. And since both sides are also monic, they must be equal.

4. $\partial - x$.

5. 1. $S = \frac{2}{2187(x-1)(x+1)(x+2)(3x+4)} D + \frac{3x+2}{729(x-1)(x+1)(x+2)(3x+4)}$, $T = \frac{3x+5}{81(x-1)(x+1)(x+2)} + \frac{1}{243(x-1)(x+1)(x+2)} D - \frac{1}{729(x-1)(x+1)(x+2)} D^2 - \frac{2}{2187(x-1)(x+1)(x+2)(3x+4)} D^3$; 2. $S = \frac{(x+6)(3x+13)}{16(x+2)(2x+7)} - \frac{x^2+12x+19}{32(x+2)(2x+7)} S - \frac{(3x+11)(x+9)}{32(x+2)(2x+7)} S^2$, $T = \frac{3x+11}{32(x+2)(2x+7)} S^4 + \frac{1}{4(x+2)} S^3 + \frac{13x+40}{16(x+2)(2x+7)} S^2 - \frac{1}{(x+2)(2x+7)} S - \frac{29x+131}{32(x+2)(2x+7)}$.

6. Let $U, V \in K[\partial]$ be coprime and suppose that there are two pairs $(S, T), (S', T') \in K[\partial]^2$ with $\operatorname{ord}(S), \operatorname{ord}(S') < \operatorname{ord}(V)$ and $\operatorname{ord}(T), \operatorname{ord}(T') < \operatorname{ord}(U)$ and $1 = SU + TV = S'U + T'V$. Then $(S - S')U + (T - T')V = 0$, which means that the vector

$$\big([\partial^0](S - S'), \ldots, [\partial^{\operatorname{ord}(V)-1}](S - S'), [\partial^0](T - T'), \ldots, [\partial^{\operatorname{ord}(U)-1}](T - T')\big)$$

in $K^{\operatorname{ord}(U)+\operatorname{ord}(V)}$ is a nonzero element of the kernel of the Sylvester matrix $\operatorname{Syl}(U, V)$. However, as was shown in the text, whenever U, V are coprime, then $\operatorname{res}(U, V) \neq 0$, so the kernel of $\operatorname{Syl}(U, V)$ is zero.

This proves the claim if U, V are coprime. If they are not and G is their greatest common right divisor, apply the argument to the two coprime operators $\operatorname{rquo}(U, G), \operatorname{rquo}(V, G)$.

7. In this case we have $G = \operatorname{lc}(U)^{-1}U$ but the only operators S, T with $\operatorname{ord}(S) < \operatorname{ord}(V) - \operatorname{ord}(G) = 0$ and $\operatorname{ord}(T) < \operatorname{ord}(U) - \operatorname{ord}(G) = 0$ are $S = T = 0$, and for these we have $SU + TV = 0 \neq G$.

8. If $r_g = \operatorname{ord}(\operatorname{gcrd}(U, V))$, then we can find the coefficients of S, T with $\operatorname{gcrd}(U, V) = SU + TV$ with $\operatorname{ord}(S) < r - r_g$ and $\operatorname{ord}(T) < r - r_g$ by solving a linear system of size $(2r - 2r_g) \times (2r - 2r_g)$ whose entries are polynomials of degree at most d. According to Theorem 1.30, this costs $\tilde{O}(r^\omega d)$ operations in C. Once we know S, T, we can compute $\operatorname{gcrd}(U, V) = SU + TV$, which costs $\tilde{O}(r^2 d)$ operations in C and is therefore negligible since $\omega \geq 2$. The assumptions on the complexity for applying σ and δ enter here. They also enter in the construction of the linear system, which also costs $\mathrm{O}^{\sim}(r^2 d)$ operations and is therefore also negligible.

We do not know r_g a priori, but we can find it by bisection search, since the linear system will have no solution if r_g is chosen to be too small and have more than one solution if r_g is too large. Since the search requires at most $\mathrm{O}(\log(r))$ probes, we stay within the required cost bound.

9. $\operatorname{gcrd}(U, V) \neq 1 \iff \operatorname{res}(U, V) = -2(\alpha-1)x(\alpha x^2 - 2\alpha x - \alpha + x^4 - 3x^2 + x + 1) \neq 0$, therefore $\alpha = 1$ is the only choice.

10. Consider the ideal $I = \langle x, D\rangle \subseteq C[x][D]$. We claim that I is not a principal left ideal. Assume otherwise. Then there are $P \in I$ and $Q_1, Q_2 \in C[x][D]$ such that $x = Q_1 P$ and $D = Q_2 P$. Since $P \in I$, we also have $U, V \in C[x][D]$ with $P = Ux + VD$. Write $U = u_0 + \cdots + u_n D^n$, $V = v_0 + \cdots + v_m D^m$ for $u_0, \ldots, u_n, v_0, \ldots, v_m \in C[x]$. Using $D^i x = xD^i + iD^{i-1}$, we find $P = (xu_0 + u_1) + (xu_1 + 2u_2 + v_0)D + (xu_2 + 3u_3 + v_1)D^2 + \cdots$, and in order to get $x = Q_1 P$, we must have $xu_1 + 2u_2 + v_0 = xu_2 + 3u_3 + v_1 = \cdots = 0$, which implies $V = -\operatorname{rquo}(Ux, D)$. Then $P = Ux + VD = \operatorname{rrem}(Ux, D) = xu_0 + u_1$ and $x = Q_1 P$ further forces $u_0 \in C \setminus \{0\}$ and $u_1 = 0$. But then also $Q_2 P$ has polynomial coefficients of degree at least 1, for any nonzero $Q_2 \in C[x][\partial]$, so we cannot have $D = Q_2 P$.

11. Without loss of generality, $\operatorname{lc}(p) = \operatorname{lc}(q) = 1$. (We already need commutativity for this step.) Since $C[x]$ a unique factorization domain, there are monic irreducible polynomials $p_1, \ldots, p_n$ and nonnegative integers $a_1, \ldots, a_n, b_1, \ldots, b_n$ such that $p = p_1^{a_1} \cdots p_n^{a_n}$ and $q = p_1^{b_1} \cdots p_n^{b_n}$. (Commutativity is needed for bringing the factors in order.) We then have $\gcd(p, q) = p_1^{\min(a_1,b_1)} \cdots p_n^{\min(a_n,b_n)}$ and $\operatorname{lcm}(p, q) = p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}$, and the claimed formula follows because we have $a + b = \min(a, b) + \max(a, b)$ for all $a, b \in \mathbb{N}$.

12. L annihilates both roots of $y^2 + ay + b$. These roots are of the form $p \pm \sqrt{q}$ for some $p, q \in C(x)$, and the assumption $a, b \neq 0$ implies $p, q \neq 0$. Then also p and $\sqrt{q}$ belong to $V(L)$, and these solutions are annihilated by $D - \frac{p'}{p}$ and $D - \frac{q'}{2q}$, respectively. Their least common left multiple has the same solution space as $V(L)$, so it must be equal to L for otherwise $\operatorname{gcrd}(L, \operatorname{lclm}(D - \frac{p'}{p}, D - \frac{q'}{2q}))$ would be an operator of order < 2 with two linearly independent solutions.

13. Let $G = \operatorname{gcrd}(U, V)$ and let $\tilde{U}, \tilde{V} \in K[\partial]$ be such that $U = \tilde{U}G$ and $V = \tilde{V}G$. We show that $\operatorname{lclm}(U, V) = \operatorname{lclm}(\tilde{U}, \tilde{V})G$. The claim then follows from Theorem 4.28 and $\operatorname{ord}(U) = \operatorname{ord}(\tilde{U}) + \operatorname{ord}(G)$ and $\operatorname{ord}(V) = \operatorname{ord}(\tilde{V}) + \operatorname{ord}(G)$, because $\operatorname{ord}(\operatorname{lclm}(U, V)) = \operatorname{ord}(\operatorname{lclm}(\tilde{U}, \tilde{V})) + \operatorname{ord}(G) \leq \operatorname{ord}(\tilde{U}) + \operatorname{ord}(\tilde{V}) + \operatorname{ord}(G) = \operatorname{ord}(U) + \operatorname{ord}(V) - \operatorname{ord}(G)$.

If T is a common left multiple of U and V, then $T = AU = BV$ for some $A, B \in K[\partial]$, thus $T = A\tilde{U}G = B\tilde{V}G$, and thus $\operatorname{rquo}(T, G)$ is a common left multiple of $\tilde{U}, \tilde{V}$. Conversely, if $\tilde{T}$ is a common left multiple of $\tilde{U}, \tilde{V}$, then $\tilde{T} = A\tilde{U} = B\tilde{V}$ for some $A, B \in K[\partial]$, thus $\tilde{T}G = AU = BV$, and thus $\tilde{T}G$ is a common left multiple of U, V.

14. If we denote G_k, S_k, T_k to be the values of G, S, T at the end of the kth iteration of the Euclidean algorithm (with $G_0 = U$, $S_0 = 1$, $T_0 = 0$), then the suggested submodule is also generated by (G_k, S_k, T_k) and $(G_{k+1}, S_{k+1}, T_{k+1})$ for any k. This is because all updates happening during the computation amount to basis changes of the module. In particular, (G, S, T) and (G', S', T') form a module basis. If $\tilde{U}, \tilde{V}$ are such that $\operatorname{lclm}(U, V) = \tilde{U}U = \tilde{V}V$, then $\tilde{U}(U, 1, 0) - \tilde{V}(V, 1, 0) = (0, \tilde{U}, -\tilde{V})$ is a module element. It must therefore be a $K[\partial]$-linear combination of (G, S, T) and (G', S', T'), and since $G \neq 0 = G'$, it must in fact be a $K[\partial]$-multiple of (G', S', T'), say $\tilde{U} = AS'$, $\tilde{V} = -AT'$ for some $A \in K[\partial]$. Since $0 = S'U + T'V$, it is clear that $S'U = -T'V$ is also a common left multiple of U and V, so by the choice of $\tilde{U}$ and $\tilde{V}$, we must have $\operatorname{ord}(A) = 0$, as claimed.

15. **a.** $\partial^3 - \frac{x^3+x+4}{x^2-x-2}\partial^2 - \frac{7x^3+10x^2+3x-4}{x^3-3x-2}\partial + \frac{6x^3+2x^2}{x^2-x-2}$; **b.** $\partial^4 + \frac{x(x+5)}{x+1}\partial^3 - \frac{x^4+x^3-2x^2+3x+1}{(x+1)^2}\partial^2 - \frac{x(5x^2+5x-2)}{x+1}\partial + 2x^3$; **c.** $(x-2)^{-2}(x+1)^{-5}(x^2+x-1)^{-1}\big((x-2)^2(x+1)^5(x^2+x-1)\partial^4 + (x-2)(x+1)^4(x^5+4x^4-12x^3-8x^2+13x-4)\partial^3 - (x+1)^2(x^9-x^8-6x^7+21x^6-30x^5-20x^4+53x^3-14x^2+46x-42)\partial^2 + (-5x^{11}-10x^{10}+30x^9+90x^8+22x^7-254x^6-192x^5+102x^4+45x^3+110x^2-72x+6)\partial + 2(x+1)^2(x^{10}-6x^8-3x^7+10x^6+5x^5-3x^4+12x^3+4x^2-16x+4)\big)$.

16. Take $F = C(x)$, $A = (x+2)^2S^2 - (2x^2+8x+7)S + (x+1)(x+3)$, $B = (x+2)S^2 - (2x+3)S + (x+1)$. Then $V(\operatorname{lclm}(A, B))$ contains x but $V(A) + V(B)$ does not. B is the minimal annihilating operator of $H_n = \sum_{k=1}^{n} \frac{1}{k}$, and A is the minimal annihilating operator of $n + H_n$.

17. The computation of $\partial^i U$ and $\partial^i V$ for $i = 0, \ldots, r$ costs altogether $O^{\sim}(r^2 d)$ operations in C by the assumptions on σ, δ. If $r_m \in \{r, \ldots, 2r\}$ is the order of $\operatorname{lclm}(U, V)$, we can make an ansatz $(s_0 + \cdots + s_{r_m-\operatorname{ord}(U)}\partial^{r_m-\operatorname{ord}(U)})U - (t_0 + \cdots + t_{r_m-\operatorname{ord}(V)}\partial^{r_m-\operatorname{ord}(V)})V = 0$. This leads to a linear system with $2r_m - \operatorname{ord}(U) - \operatorname{ord}(V)$ variables and equations, and with polynomial coefficients of degree at most d. A nullspace basis of such a system can be computed with $O^{\sim}(r^{\omega}d)$ operations in C by Theorem 1.30.

We do not know r_m a priori, but we can find it with a bisection search, since the linear system will have no solution if r_m is chosen too small and more than one solution if r_m is too large. Finding the right r_m requires no more than $O(\log(r))$ probes.

Algorithm 4.27 has the asymptotic complexity $O^{\sim}(r^{\omega+1}d)$ since it does not do a bisection search, but it tends to perform better for problem sizes typically encountered in practice, in particular in combination with homomorphic images. A more careful analysis of algorithms for common left multiples can be found in [88].

18. Let $Q \in C(x)[\partial]$ be any p^k-removing operator of order n for P. Then we have $\operatorname{lc}(QP) \mid \sigma^n(\operatorname{lc}(P)/p)$, by definition of removability, and we may in fact assume

$\operatorname{lc}(QP) = \sigma^n(\operatorname{lc}(P)/p)$ by multiplying Q from the left by a suitable polynomial, if needed. Now let $q \in C[x]$ be such that $\gcd(q, \sigma^n(p)) = 1$ and let $s, t \in C[x]$ be such that $sq + t\sigma^n(p) = 1$. Let $U \in C[x][\partial]$ be such that $\operatorname{ord}(U) < n$. Then $\tilde{Q} := sqQ + t\partial^n + U$ is also a p^k-removing operator of order n for P, because $\operatorname{lc}(\tilde{Q}P) = sq\operatorname{lc}(QP) + t\sigma^n(\operatorname{lc}(P)) = (sq + t\sigma^n(p))\sigma^n(\operatorname{lc}(P)/p)$ and $\tilde{Q}P \in C[x][\partial]$. By choosing suitable $q \in C[x]$ and $U \in C[x][\partial]$, we can ensure that $\tilde{Q}$ has the required form. More precisely, we choose q such as to clear all factors from the denominators of Q that are coprime to p, and U so that that $[\partial^i]U = -\operatorname{quo}([\partial^i]sqQ, \sigma^n(p)^{e_i})$ for $i = 0, \dots, n-1$.

19. Let $Q_1, Q_2 \in C(x)[\partial]$ be such that $Q_iP \in C[x][\partial]$ and $\operatorname{ord}(Q_i) = n$ and $\operatorname{lc}(Q_iP) \mid \sigma^n(\operatorname{lc}(P)/p_i)$ for $i = 1, 2$. By multiplying the Q_i from the left with suitable elements of $C[x]$, if necessary, we may in fact assume that $\operatorname{lc}(Q_iP) = \sigma^n(\operatorname{lc}(P)/p_i)$ for $i = 1, 2$. Let $q_1, q_2 \in C[x]$ be such that $q_1\sigma^n(p_1) + q_2\sigma^n(p_2) = \gcd(\sigma^n(p_1), \sigma^n(p_2))$ and define $Q = q_2Q_1 + q_1Q_2$. Then

$$\begin{aligned}\operatorname{lc}(QP) = q_2\operatorname{lc}(Q_1P) + q_1\operatorname{lc}(Q_2P) &= \frac{q_2\sigma^n(p_2) + q_1\sigma^n(p_1)}{p_1p_2}\sigma^n(\operatorname{lc}(P))\\ &= \frac{\gcd(\sigma^n(p_1), \sigma^n(p_2))}{p_1p_2}\sigma^n(\operatorname{lc}(P)) = \sigma^n(\operatorname{lc}(P)/\operatorname{lcm}(p_1, p_2)).\end{aligned}$$

The claim follows.

20. **a.** $D + x$, we have $U = (D + x)(D - x)$ and $V = (D + x)(xD - 2)$; **b.** $L = D^3 - \frac{2(x^2-6)}{x(x^2-3)}D^2 - \frac{x^8-5x^6-x^4+69x^2-72}{x^2(x^2-3)^2}D + \frac{2(x^10-11x^8+31x^6+45x^4-162x^2+108)}{x^3(x^2-3)^3}$, we have $L = U(D - \frac{2(x^2-6)}{x(x^2-3)}) = V(\frac{1}{x}D - \frac{x^4-4x^2-3}{x^2(x^2-3)})$.

21. False. For example, for $U = D^2$, $V = (D - 1)(xD - 1) \in C(x)[D]$ we have $\operatorname{gcrd}(U, V) = D - \frac{1}{x}$ while the greatest common left divisor is 1.

22. No. If $r \in C(x)$ is such that $r(n) = h_{n+1}/h_n$, then the d'Alembertian solution is annihilated by $(S - 1)(S - r)$. Every other recurrence operator which has this solution must have a common right factor with $(S - 1)(S - r)$. The common right factor may have order one or order two. If it has order one, then $\sum_{k=1}^n h_k$ is itself hypergeometric, and then it must be similar to h_n. If it has order two, it must be $(S - 1)(S - r)$, and then $S - r$ is also a right factor, so h_n is a solution.

Section 4.3

1. Let $A = ((a_{i,j}))_{i,j=1}^r$, $B = ((b_{i,j}))_{i,j=1}^r \in K^{r\times r}$. It is clear that $\sigma(A + B) = \sigma(A) + \sigma(B)$ and $\delta(A + B) = \delta(A) + \delta(B)$. Since we have $\sigma(\sum_{k=1}^r a_{i,k}b_{k,j}) = \sum_{k=1}^r \sigma(a_{i,k})\sigma(b_{k,j})$ for all i and j, we have $\sigma(AB) = \sigma(A)\sigma(B)$, so $\sigma\colon K^{r\times r} \to K^{r\times r}$ is an endomorphism. Next, from $\delta(\sum_{k=1}^r a_{i,k}b_{k,j}) = \sum_{k=1}^r \delta(a_{i,k}b_{k,j}) =$

$\sum_{k=1}^{r} \delta(a_{i,k})b_{k,j} + \sum_{k=1}^{r} \sigma(a_{i,k})\delta(b_{k,j})$ we get $\delta(AB) = \delta(A)B + \sigma(A)\delta(B)$, so $\delta\colon K^{r\times r} \to K^{r\times r}$ is a σ-derivation.

2. a. $I_r = \sigma(I_r) = \sigma(AA^{-1}) = \sigma(A)\sigma(A)^{-1}$ implies $\sigma(A)^{-1} = \sigma(A^{-1})$. **b.** $0 = \delta(I_r) = \delta(A^{-1}A) = \delta(A^{-1})A + \sigma(A^{-1})\delta(A)$ implies $\delta(A^{-1}) = -\sigma(A^{-1})\delta(A)A^{-1}$.

3. By the theorem of Cayley-Hamilton, the characteristic polynomial $\chi = \det(A - xI_r) \in C[x]$ of A has the property $\chi(A) = 0$. From $(I_r\partial - A)\cdot f = 0$ we get $\partial f = Af$, and since $\sigma = \mathrm{id}$ and $\delta = 0$, it follows $\chi(\partial)f = \chi(A)f = 0$, so we can take $L = \chi(\partial)$.

4. Consider an invertible matrix $Y \in C(x)^{r\times r}$ whose entries are C-linearly independent. Such matrices clearly exist. For example, we can start from an invertible matrix in $C^{r\times r}$ and multiply the (i, j)-th entry by x^{i+rj}, for all $i, j = 1, \ldots, r$. The matrix $A = Y'Y^{-1}$ is then so that the columns of Y form a vector space basis of the solution space of the system $(I_r D - A)\cdot f = 0$. Since the desired operator L must annihilate each component of Y and the components are chosen to be C-linearly independent, the order of L must be at least r^2.

5. Suppose that $f, g \in F$ are annihilated by $L, M \in K[S] \setminus \{0\}$, respectively. Let $C_L \in K^{r\times r}$ and $C_M = ((c_{M,i,j}))_{i,j=1}^{s} \in K^{s\times s}$ be the companion matrices of L, M and consider the matrix

$$A = C_L \otimes C_M = \begin{pmatrix} C_L c_{M,1,1} & \cdots & C_L c_{M,1,s} \\ \vdots & \ddots & \vdots \\ C_L c_{M,s,1} & \cdots & C_L c_{M,s,s} \end{pmatrix} \in K^{rs\times rs}.$$

For the vector $h = (\sigma^{k \bmod r}(f)\sigma^{\lfloor k/r\rfloor}(g))_{k=0}^{rs-1} \in F^{rs}$ we then have $\sigma(h) = Ah$, and Proposition 4.34 implies that every component of h, in particular its first component fg, are D-finite.

6. An inverse is $\frac{1}{x(x+1)(x+2)}\begin{pmatrix} -xS + x^2(x+2) & xS^2 + -x(x^2+2x-1)S + x(x+2) \\ x+2 & (-x-2)S - x - 2 \end{pmatrix}$.

7. a. $A^{-1} \in K^{r\times r} \subseteq K[\partial]^{r\times r}$ is an inverse. **b.** A^{-1} is the matrix which is defined in the same way as A but with $-L$ in place of L.

8. In both cases, a basis of the solution space is $\{\begin{pmatrix} 1 \\ 3 \\ -x \end{pmatrix}, \begin{pmatrix} 1/x \\ 0 \\ 1 \end{pmatrix}\}$.

9. Let $Y \in C(x)^{3\times 3}$ be the matrix whose columns are the three given basis vectors. We need a matrix $A \in C(x)^{3\times 3}$ such that $Y' = AY$. Obviously the matrix $A = Y'Y^{-1}$ does the job.

10. Since there is a unimodular matrix U with $UH = (G, 0, \ldots, 0)$, the entries of A generate the same left ideal in $K[\partial]$ as G. The claim follows by repeated application of Theorem 4.24.

11. **a.** If H is the Hermite normal form of $I_r\partial - A \in K[\partial]^{r\times r}$ and $U \in K[\partial]^{r\times r}$ is a unimodular matrix such that $U(\partial I_r - A) = H$, then the system $(I_r\partial - A)\cdot f = c_1 g_1 + \cdots + c_m g_m$ is equivalent to the system $H\cdot f = c_1(U\cdot g_1) + \cdots + (U\cdot g_m)$, which we can solve from the bottom up like in the homogeneous case. **b.** $(f, c_1, \ldots, c_m) \in K^r \times C^m$ is a solution of the system of interest if and only if $(Pf, c_1, \ldots, c_m)$ is a solution of the system $(I_r\partial - P[A])\cdot \tilde{f} = c_1\tilde{g}_1 + \cdots + c_m\tilde{g}_m$ with $\tilde{g}_i = \sigma(P)g_i$ $(i = 1, \ldots, m)$.

12. Reflexivity: $I_n[A] = A$. Transitivity:

$$\begin{aligned}
P_1[P_2[A]] &= P_1[(\sigma(P_2)A + \delta(P_2))P_2^{-1}]\\
&= (\sigma(P_1)(\sigma(P_2)A + \delta(P_2))P_2^{-1} + \delta(P_1))P_1^{-1}\\
&= (\sigma(P_1P_2)A + \sigma(P_1)\delta(P_2) + \delta(P_1)P_2)(P_1P_2)^{-1}\\
&= (\sigma(P_1P_2)A + \delta(P_1P_2))(P_1P_2)^{-1}\\
&= (P_1P_2)[A].
\end{aligned}$$

Symmetry: by $P^{-1}[P[A]] = (P^{-1}P)[A] = A$.

13. The question is whether there is an invertible matrix $P \in K^{r\times r}$ such that $(PA + P')P^{-1} = B$, i.e., $PA + P' = PB$, i.e., $P' = P(B - A)$. This is the case if and only if there are r linearly independent vectors $p \in K^r$ with $p' = p(B - A)$, or, if we prefer to view them as column vectors, with $p' = (B - A)p$. Whether this is the case can be determined by solving this system with the methods described in this section.

14. **a.** False. What is true is that the $C(x)$-vector spaces generated by the solutions of two gauge equivalent systems agree, but the solution spaces themselves are only C-vector spaces and differ in general. **b.** False. For example, in the differential case with $K = C(x)$, we have

$$\begin{pmatrix} 1 & x-1 \\ 0 & x+1 \end{pmatrix}[\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} 0 & 1 \\ 0 & -\frac{x+2}{x+1} \end{pmatrix}.$$

Note that the operator $D^2 - D$ has the solutions 1 and $\exp(x)$ while the operator $D^2 + \frac{x+2}{x-1}D$ has the solutions 1 and $x\exp(x)$. **c.** False. For example, in the differential case with $K = C(x)$ we can take $p = (1, x, x^2, \ldots, x^{r-1})$. Defining $p_1 = p$ and $p_k = p_{k-1} + p'_{k-1}$ for $k > 1$, the matrix $P \in C(x)^{r\times r}$ with rows $p_1, \ldots, p_r$ is equivalent to the matrix $\tilde{P}$ whose rows are $p, p', p'', \ldots$, which is an upper triangular matrix whose diagonal entries are $1, 2, 6, \ldots, r!$, and their product is nonzero. Thus, the $p_1, \ldots, p_r$ are linearly independent.

15. For $1 < i \le n$ we have $\sigma(e_{i-1})A + \delta(e_{i-1}) = e_{i-1}A = e_i$ when A has the form of a companion matrix, and since $e_1, \ldots, e_n$ are linearly independent, the claim follows. For the other direction, we can for example take a companion matrix with $r > 2$ and permute the first $r-1$ rows in order to destroy the companion matrix structure. For the resulting matrix, e_1 will still be a cyclic vector.

16. Let $\phi\colon K^r \to K[\partial]/\langle L\rangle$ be the K-linear map defined by $\phi(e_i) = [\partial^{i-1}]$ ($i = 1, \dots, r$). It suffices to show that ϕ commutes with ∂. Indeed, by the design of the companion matrix, we have $\phi(\partial\cdot e_i) = \phi(e_{i+1}) = [\partial^i] = \partial\cdot[\partial^{i-1}] = \partial\cdot\phi(e_i)$ for $i = 1, \dots, r-1$. The last row of the companion matrix contains the coefficients of $\operatorname{rrem}(\partial^r, L)$, which implies that also $\partial\cdot\phi(e_r) = \partial\cdot[\partial^{r-1}] = [\partial^r] = [\operatorname{rrem}(\partial^r, L)] = \phi(\partial\cdot e_r)$.

17. The assumption on F also implies that a parameterized equation $Lf = c_1 g_1 + \dots + c_m g_m$ with given $L \in K[\partial]$ of order r and given $g_1, \dots, g_m \in F$, and with unknown $f \in F$ and unknown $c_1, \dots, c_m \in C$, has a solution space in $F \times C^m$ of dimension at most $r + m$.

Without loss of generality, we may assume that A has the form produced by Algorithm 4.44, say with blocks of sizes $r_1, \dots, r_k$ with $r_1 + \dots + r_k = r$. The first block translates into an equation $L_1 f_1 = 0$, which by assumption has a solution space of dimension $d_1 \le r_1$. The second block translates into an equation $L_2 f_2 = M_{2,1} f_1$, which we can view as a parameterized equation with d_1 components on the right. Its solution space has dimension $d_2 \le r_2 + d_1 \le r_1 + r_2$. In the next step, $L_3 f_3 = M_{3,1} f_1 + M_{3,2} f_2$ is a parameterized equation whose right hand side has d_2 degrees of freedom (each basis element of the solution space of the second equation gives rise to a pair (f_1, f_2)). By induction, we see that the ith block ($i = 1, \dots, k$) translates into a parameterized equation whose solution space has dimension $r_1 + \dots + r_i$. The claim follows.

18. Write $A = ((\sum_{n=0}^\infty a_{i,j,n} x^n))_{i,j=1}^r$ and consider a vector $f = (f_1, \dots, f_r) \in C[[x]]^r$ with $f_i = \sum_{n=0}^\infty f_{i,n} x^n$. In order for f to be a solution of the system, it is necessary and sufficient that $[x^n]f' = [x^n]Af$ for all $n \in \mathbb{N}$. Coefficient extraction leads to a coupled recurrence system

$$\begin{pmatrix}(n+1) f_{1,n+1}\\ \vdots \\ (n+1) f_{r,n+1}\end{pmatrix} = \begin{pmatrix}\sum_{j=1}^r \sum_{k=0}^n a_{1,j} f_{j,k}\\ \vdots \\ \sum_{j=1}^r \sum_{k=0}^n a_{r,j} f_{j,k}\end{pmatrix}.$$

With this system, every choice $(f_{1,0}, \dots, f_{r,0}) \in C^r$ of initial terms can be uniquely extended to a vector $f \in C[[x]]^r$ with $(I_r D - A)\cdot f = 0$.

19. The solution space of the system is generated by $\binom{1}{0}$ and $\binom{\log(x)}{1}$. Consider a matrix $P \in C[x]^{2\times 2}$ which is invertible in $C(x)^{2\times 2}$. Then $P\binom{\log(x)}{1}$ also contains logarithmic terms, so the system $(I_2 D - P[A])\cdot f = 0$ has at least one solution which does not have only power series coefficients. If $P[A]$ were an element of $C(x)^{2\times 2}$ with entries whose denominators do not contain x, so that $P[A]$ can be viewed as element of $C[[x]]^{2\times 2}$, then Exercise 18 implies that there are two linearly independent solutions in $C[[x]]^2$, which together with the solution involving logarithmic terms makes three linearly independent solutions in $C((x))[\log x]^2$. By Exercise 17, this is impossible.

20. **a.** We use $\operatorname{lclm}(P, A) = P[A]P$. For $f \in V(A)$ we have $P[A] \cdot (P \cdot f) = P[A]P \cdot f = \operatorname{lclm}(P, A) \cdot f = 0$, so $P \cdot f \in V(P[A])$. Having thus shown that $P \cdot V(A) \subseteq V(P[A])$, we can view P as a C-linear map $V(A) \to V(P[A])$. Its kernel is $V(A) \cap V(P) = V(\operatorname{gcrd}(A, P))$, and because of $\dim \operatorname{im} P = \dim V(A) - \dim \ker P = \operatorname{ord}(A) - \operatorname{ord}(\operatorname{gcrd}(A, P)) = \operatorname{ord}(\operatorname{lclm}(P, A)) - \operatorname{ord}(P) = \operatorname{ord}(P[A])$, the map P is surjective. We therefore also have $P \cdot V(A) \supseteq V(P[A])$. **b.** $V(P[\operatorname{lclm}(A, B)]) = P \cdot V(\operatorname{lclm}(A, B)) = P \cdot (V(A) + V(B)) = (P \cdot V(A)) + (P \cdot V(B)) = V(P[A]) + V(P[B]) = V(\operatorname{lclm}(P[A], P[B]))$. Since $P[\operatorname{lclm}(A, B)]$ and $\operatorname{lclm}(P[A], P[B])$ are both monic and have the same solution space, the assumption on the ambient module F implies that the operators are identical. **c.** "$\Rightarrow$": Let $S, T \in K[\partial]$ be such that $SP + TA = 1$. Then P maps $V(A)$ to $V(P[A])$, and SP acts as identity on $V(A)$, so S maps $V(P[A])$ to $V(A)$. Therefore $\dim V(A) = \dim V(P[A])$ and therefore $\operatorname{ord}(A) = \operatorname{ord}(P[A])$. "$\Leftarrow$": $\operatorname{ord}(A) = \operatorname{ord}(P[A]) = \operatorname{ord}(\operatorname{lclm}(P, A)) - \operatorname{ord}(P)$ implies $\operatorname{ord}(\operatorname{gcrd}(P, A)) = \operatorname{ord}(A) + \operatorname{ord}(P) - \operatorname{ord}(\operatorname{lclm}(P, A)) = 0$, so $\operatorname{gcrd}(P, A) = 1$.

21. Plug the ansatz into the differential equation for $f(x)$ and use the differential equation for the Bessel function (with $\nu = 2$) in order to rewrite the resulting expression as a linear combination of J_2 and J_2'. Equating their coefficients to zero gives the coupled system

$$\begin{aligned}
&x(2x-1)(10x+9)u''(x) + 2(50x^2+39x-18)u'(x) + \frac{86x^2+131x-36}{x}u(x)\\
&\quad - \frac{2(x-2)(x+2)(2x-1)(10x+9)}{x}v'(x)\\
&- \frac{80x^4+70x^3-187x^2-216x+36}{x^2}v(x) = 0,\\
&x(2x-1)(10x+9)v''(x) + 2(30x^2+31x-9)v'(x) + \frac{26x^2+69x-18}{x}v(x)\\
&\quad + 2x(2x-1)(10x+9)u'(x) + (80x^2+70x-27)u(x) = 0.
\end{aligned}$$

The system turns out to have the solution $(u, v) = (\frac{3x+2}{x^2(2x-1)}, \frac{1}{x(2x-1)})$, giving rise to the solution $f(x) = \frac{3x+2}{x^2(2x-1)} J_2(x) + \frac{1}{x(2x-1)} J_2'(x)$ of the differential equation.

See [169, 449] for algorithms that solve differential equations in terms of Bessel functions in a more general sense.

22. Choose a basis $\{b_1, \ldots, b_r\}$ of K and make an ansatz $g = g_1 b_1 + \cdots + g_r b_r$ with undetermined coefficients $g_i \in C(x)$. Forcing $g' = g_1' b_1 + g_1 b_1' + \cdots + g_r' b_r + g_r b_r' = f$ and equating coefficients of $b_1, \ldots, b_r$ on both sides gives an inhomogeneous first order system of differential equations over $C(x)$ for the unknown rational functions $g_1, \dots, g_r$. This system can be solved with the methods presented in this section.

23. We may assume without loss of generality that all quasi-polynomials are expressed in terms of the same root of unity ω. (If there are several distinct ones, we can take as ω a generator of the multiplicative group generated by all the roots of unity.)

If ω is a kth root of unity, then for every $i \in \mathbb{N}$ the subsequences $(p^{(0)}_{kn+i})_{n=0}^{\infty}, \dots, (p^{(r)}_{kn+i})_{n=0}^{\infty}$ are in fact polynomial sequences.

Section 4.4

1. If $c \neq 0$, the solution space of L is generated by c^x and xc^x. Any first order factor of L must annihilate a certain linear combination $(\alpha + \beta x)c^x$, and for each choice $(\alpha, \beta) \neq (0, 0)$, such a factor is given by $(\alpha + \beta x)S - c(\alpha + \beta + \beta x)$. For $c = 0$, we claim that $L = S^2$ is the only factorization. Indeed, if $S - q(x)$ is a right factor, then $\operatorname{rrem}(S^2, S - q(x)) = q(x)q(x + 1)$, which is only zero if $q(x)$ is zero.

2. No. For example, $(xD + 1)D$ is the minimal order annihilating operator of $\log(x)$. It can also be that the minimal order annihilating operator is an lclm, cf. Exercise 12 of Sect. 4.2.

3. Both maps are evidently K-vector space isomorphisms. What remains to be shown is that they commute with D. For the map $\phi\colon M_1 \to N_1$ and an element $[qD] \in M_1$ ($q \in C(x)$), we have $\phi(D \cdot [qD]) = \phi([DqD]) = \phi([(qD+q')D]) = \phi([qD^2 + q'D]) = \phi([q'D]) = [(x - 1)q'D - q']$ and $D \cdot \phi([qD]) = D \cdot [(x - 1)qD - q] = [D(x - 1)qD - Dq] = [(q + (x - 1)q')D - (qD + q')] = [(x - 1)q'D - q']$. If ψ denotes the other map, then for any element $[q]$ ($q \in C(x)$) we have $\psi(D\cdot[q]) = \phi([Dq]) = \phi([qD+q']) = \phi([q']) = [\frac{1}{x-1}q']$ and $D\cdot\psi([q]) = D \cdot [\frac{1}{x-1}q] = [D\frac{1}{x-1}q] = [\frac{1}{x-1}qD - \frac{1}{(x-1)^2}q + \frac{1}{x-1}q'] = [\frac{1}{x-1}q\frac{1}{x-1} - \frac{1}{(x-1)^2}q + \frac{1}{x-1}q'] = [\frac{1}{x-1}q']$.

4. Because of the isomorphism and the fact that L is irreducible if and only if $K[\partial]/\langle L\rangle$ is simple, it suffices to show that the module K^r has a nontrivial submodule if and only if it has a nonzero non-cyclic vector.

"$\Rightarrow$": If M is a nontrivial submodule and p is a nonzero element of M, then the vectors $p, \partial \cdot p, \dots \in K^r$ generate a K-vector space of dimension at most $\dim_K(M) < r$, so p is not a cyclic vector. "$\Leftarrow$": If $p \in K^r$ is a nonzero non-cyclic vector, then $p, \partial \cdot p, \dots \in K^r$ generate a K-vector space $M \subseteq K^r$ with $\dim_K(M) < r$. This vector space is closed under application of ∂ and therefore is a nontrivial submodule.

5. $((x + 2)S - (x + 1))(S - 1)$ is obviously reducible, but it is not completely reducible because it has a generalized series solution involving a logarithmic term, and if it were completely reducible, it would have two linearly independent hypergeometric solutions, corresponding to series solutions that cannot involve logarithmic terms.

6. If $y_1, \ldots, y_r \in E$ form a basis of $V(L)$, we have $L = \mathrm{lc}(L)\,\mathrm{lclm}(D - y_1'/y_1, \ldots, D - y_r'/y_r)$.

7. False. A counter example is given by the operator $L = (D - x)(D^2 - x) \in C(x)[\partial]$, which has no first order right factors. Therefore, for every chain $\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 = C(x)[\partial]/\langle L\rangle$ we have $\dim_K M_1/M_0 = 2$ and $\dim_K M_2/M_1 = 1$, while for the claim to be true we would also need a chain $\{0\} = N_0 \subsetneq N_1 \subsetneq N_2 = C(x)[\partial]/\langle L\rangle$ with $\dim_K N_1/N_0 = 1$ and $\dim_K N_2/N_1 = 2$.

8. **a.** False. To construct a counterexample, choose an algebraic function y and let L_1 be an annihilating operator of y and L_2 be an annihilating operator of $1/y$. Unless y was chosen too simple, L_1, L_2 will be irreducible. The symmetric product $L_1 \otimes L_2$ will have the solution 1, so it will contain the right factor D. For example, let y be defined by $y^5 + xy^2 - 1 = 0$. Then $L_1 = (108x^7 - 3125x^2)D^4 + (1134x^6 + 6250x)D^3 + (2706x^5 - 6250)D^2 + 1080x^4 D - 72x^3$, $L_2 = (108x^6 - 3125x)D^4 + (1242x^5 + 3125)D^3 + 3210x^4 D^2 + 1140x^3 D - 132x^2$. It can be checked that L_1, L_2 are irreducible. However, $L_1 \otimes L_2$ contains the right factor D. **b.** False. Take for example $P_1 = D - 1/(x-1)$, $P_2 = D - 1/(x-2)$, $P_3 = D - 1/(x-3) \in C(x)[D]$. **c.** False. Take for example $L = \mathrm{lclm}(L_1, L_2)$ with $L_1 = (x-1)xD - (4x+3)$ and $L_2 = x(x^2+x+1)D + (x^2+2x+3)$. Then $V(L_1)$ is generated by $x^{-3}(1-x)^{-1} = x^{-3} + x^{-2} + x^{-1} + 1 + x + \cdots$ and $V(L_2)$ is generated by $x^{-3} + x^{-2} + x^{-1}$, so neither of them contains a formal power series. However $V(L) = V(L_1) + V(L_2)$ contains the formal power series $1 + x + x^2 + \cdots$.

9. In the commutative case, for any pairwise distinct monic irreducible polynomials $P_1, \ldots, P_m \in C[\partial]$ we have $\mathrm{lclm}(P_1, \ldots, P_m) = P_1 \cdots P_m$. The claim follows immediately from here. This exercise appears as part 3 of Example 2.39 in [441].

10. The set $I = \{\, P \in K[\partial] : [P] \in M \,\}$ is a left ideal of $K[\partial]$, and because of the Euclidean algorithm (cf. Sect. 4.2), every left ideal of $K[\partial]$ is generated by a single element G. The class $[G] \in K[\partial]/\langle L\rangle$ is a generator of M.

11. Let M_1, M_2 be the submodules generated by $[S - x]$ and $[S - x^2]$, respectively. Because of $1 = \frac{1}{x^2-x}(S - x) - \frac{1}{x^2-x}(S - x^2)$, we have $M_1 + M_2 = C(x)[S]/\langle \mathrm{lclm}(S - x, S - x^2)\rangle$. Because of $\mathrm{rrem}(S(S-x), \mathrm{lclm}(S-x, S-x^2)) = \frac{x^2(x+1)}{x-1}(S - x)$, the module M_1 consists just of the $C(x)$-multiples of $S - x$, and because of $\mathrm{rrem}(S(S-x^2), \mathrm{lclm}(S-x, S-x^2)) = \frac{x(x+1)}{x-1}(S - x^2)$, the module M_2 consists just of the $C(x)$-multiples of $S - x^2$. Therefore, $\dim_K(M_1) = \dim_K(M_2) = 1$, which together with $\dim_K(M_1 + M_2) = 2$ implies $M_1 \cap M_2 = \{0\}$, so the sum is direct.

12. Let $L \in K[\partial]$ and let E_L be its eigenring. It is clear that $[1]$ belongs to E_L. Let $P, Q \in K[\partial]$ be such that $[P], [Q] \in E_L$, i.e., such that $[\partial P] = [P\partial]$ and $[\partial Q] = [Q\partial]$. Adding both equations directly gives $[\partial(P + Q)] = [(P + Q)\partial]$, so E_L is closed under addition. For the product, let $\tilde{P}, \tilde{Q} \in K[\partial]$ be such that $\partial P - P\partial = \tilde{P}L$ and $\partial Q - Q\partial = \tilde{Q}L$. Multiply the first equation from the right by Q and the second from the left by P, and add the results. This gives $\partial PQ - PQ\partial = \tilde{P}LQ + P\tilde{Q}L$. Since Q is an element of the eigenring, we have $\operatorname{rrem}(LQ, L) = 0$, the right hand side is a left multiple of L, so we have $[\partial PQ] = [PQ\partial]$, and E_L is closed under addition.

It remains to show that addition and multiplication are well defined. For the addition, this is easy to see. For the multiplication, let $P', Q' \in K[\partial]$ be such that $P - P' = \tilde{P}L$ and $Q - Q' = \tilde{Q}L$ for certain $\tilde{P}, \tilde{Q} \in K[\partial]$. Multiply the first equation from the right with Q and the second from the left with P' and add the results. This gives $PQ - P'Q' = \tilde{P}LQ + P'\tilde{Q}L$, and as before, $\operatorname{rrem}(LQ, L) = 0$ implies that the right hand side is a multiple of L, so $[PQ] = [P'Q']$.

13. It suffices to show that any submodule of a semi-simple module is semi-simple. Indeed, let M be semi-simple and N be a submodule of M. If U is a submodule of N, it is also a submodule of M, so there exists a submodule $\tilde{U}$ of M such that $M = U \oplus \tilde{U}$. We then have $N = U \oplus (\tilde{U} \cap N)$.

14. As h is defined by the image of a generator, it is clearly a homomorphism. By $h(\tilde{\partial}) = \alpha\partial - \partial\alpha = (\alpha - \sigma(\alpha))\partial - \delta(\alpha)$ and $\sigma(\alpha) \neq \alpha$, the inverse of h is given by $h^{-1}(\partial) = \frac{1}{\alpha - \sigma(\alpha)}\tilde{\partial} - \delta(\alpha)$, so h is indeed bijective.

For every $p \in K$, we have $\tilde{\partial}p = (\alpha\partial - \partial\alpha)p = \alpha\partial p - \partial(\alpha p) = \alpha\sigma(p)\partial + \alpha\delta(p) - \sigma(p)\partial\alpha - \delta(p)\alpha = \sigma(p)(\alpha\partial - \partial\alpha) = \sigma(p)\tilde{\partial}$, so $\tilde{\delta} = 0$ as required.

15. It is clear that $(A + B)^* = A^* + B^*$ for all $A, B \in K[\partial]$. Therefore, it suffices to consider the case $P = p_i\partial^i$ and $Q = q_j\partial^j$, i.e., it suffices to show $(p_i\partial^i q_j\partial^j)^* = (q_j\partial^j)^*(p_i\partial^i)^*$. It is also clear from the definition that $(pB)^* = B^*p$ and $(A\partial)^* = \partial^*A^*$ for any $p \in K$ and $A, B \in K[\partial]$. So it actually suffices to show $(\partial^i q)^* = q(\partial^*)^i$ for all $i \in \mathbb{N}$ and all $q \in K$. This is obviously true for $i = 0$. Now let i be such that $(PQ)^* = Q^*P^*$ is true for all operators of order less than i. Then $(\partial^i q)^* = (\partial^{i-1}\partial q)^* = (\partial q)^*(\partial^*)^{i-1} = (\sigma(q)\partial + \delta(q))^*(\partial^*)^{i-1} = (\partial^*\sigma(q) + \delta(q))(\partial^*)^{i-1} = (\sigma^*(\sigma(q))\partial^* + \delta^*(\sigma(q)) + \delta(q))(\partial^*)^{i-1} = q\partial^*\partial^*(\partial^*)^{i-1} = q(\partial^*)^{i-1}$, as required.

For the second claim, consider an operator $P = p\partial^i$, so that $P^* = (\partial^*)^i p$. By the first claim, we have $P^{**} = ((\partial^*)^i p)^* = p^*((\partial^*)^i)^*$, and since $p^* = p$ and $((\partial^*)^i)^* = (\partial^{**})^i = \partial^i$, the claim follows. Note that the identification of ∂^{**} with ∂ is justified by $\sigma^{**} = \sigma$ and $\delta^{**} = \delta$, which follow directly from the definition.

16. For the hint, let K be an algebraic extension of $C(x)$ containing f and all its conjugates. Every $g \in K$ has the annihilating operator $gD - g \in K[D]$, and if $L \in K[D]$ is the least common left multiple $K[D]$ of all the operators $gD - g \in K[D]$, where g runs through the conjugates of f, then L obviously has only algebraic solutions, because its solution space is generated by the conjugates of f. Since the least common left multiple is invariant under permuting its arguments, its coefficients are symmetric functions in the conjugates of f, and therefore belong to $C(x)$. Thus the operator L is as required by the hint.

To show the main claim, let $P \in C(x)[D]$ be irreducible and suppose that it has a nonzero algebraic solution f. By the hint, there is an operator $L \in C(x)[D]$ with

$L \cdot f = 0$ and which only has algebraic solutions. Then f is also a solution of $\mathrm{gcrd}(P, L)$, so $\mathrm{gcrd}(P, L) \neq 1$, so P and L have a common right divisor. Since P is irreducible, this can only mean that L is a left multiple of P. This in turn means that every solution of P is a solution of L, so every solution of P is algebraic.

17. $D \in K[\partial]$ is a common right divisor of A, B iff there are $\tilde{A}, \tilde{B}$ such that $A = \tilde{A}D$, $B = \tilde{B}D$ iff there are $\tilde{A}, \tilde{B}$ such that $A^* = D^*\tilde{A}^*$, $B^* = D^*\tilde{B}^*$ iff D^* is a common left divisor of A^*, B^*. The claim follows.

18. If $\delta = 0$, we have $[\partial^0](PQ) = ([\partial^0]P)([\partial^0]Q)$, so if $L = P_1 \cdots P_m$ is a factorization of L, then $0 = [\partial^0]L = \prod_{i=1}^m [\partial^0]P_i$ implies that $\mathrm{rrem}(P_i, \partial) = 0$ for at least one i. Since P_i is monic and irreducible, $P_i = S$ is the only possibility. A counterexample for the case $\sigma = \mathrm{id}$, $\delta \neq 0$ is the factorization of D^2 stated in the text.

19. L annihilates every element of $V(\mathrm{lclm}(U, V))$, thus $\mathrm{rrem}(L, \mathrm{lclm}(U, V))$ annihilates every element of $V(\mathrm{lclm}(U, V))$. By the global assumptions of this section, $\dim_C V(\mathrm{lclm}(U, V)) = \mathrm{ord}(\mathrm{lclm}(U, V))$, so $\mathrm{rrem}(L, \mathrm{lclm}(U, V))$ is an operator of order $< \mathrm{ord}\,\mathrm{lclm}(U, V)$ with $\mathrm{ord}(\mathrm{lclm}(U, V))$ linearly independent solutions. Hence, it must be the zero operator.

20. **a.** $\mathrm{lclm}(D^3 + xD + 1, D^2 - 2x)$; **b.** $\mathrm{lclm}(D^2 - xD + 1, D^2 + D - x)$; **c.** $\mathrm{lclm}(S^2 - xS + 1, S^2 + S - x)$; **d.** $\mathrm{lclm}(S^2 - S + x, S^2 + S - x)$.

21. Write $Y = ((\theta^{i+1}(y_j)))_{i,j=0}^{r-1}$, so that $\theta(Y) = C_L Y$, where C_L is the companion matrix of L. **a.** Applying the determinant on both sides gives the desired result. Note that det and σ commute. **b.** det and δ do not commute, but by the definition of the determinant and the product rule, we can write $\delta(W(y_0, \ldots, y_{r-1})) = \sum_{i=0}^{r-1} W_i$ where W_i is the determinant obtained from $W(y_0, \ldots, y_{r-1})$ obtained by applying δ to the ith row. For every $i \leq r-1$, this yields a determinant with two identical rows, which therefore is zero. We therefore just have $\delta(W(y_0, \ldots, y_{r-1})) = W_{r-1}$. In this latter determinant, replace every occurrence of $\delta^r(y_j)$ by $\ell_{r-1}\delta^{r-1}(y_j) + \cdots + \ell_0 y_j$ ($j = 0, \ldots, r-1$), then use the rows $0, \ldots, r-2$ to eliminate the terms $\ell_{r-2}\delta^{r-2}(y_j) + \cdots + \ell_0 y_j$ and pull out the factor ℓ_{r-1} to obtain the desired equation. **c.** See the solution of Exercise 19 in Sect. 2.2.

22. No. For example, the operator $L = xD - 1$ is irreducible, and as $V(L)$ is generated by the identity function, M is simply the minimal order annihilating operator for g in this case. The algebraic function $g = 1 + \sqrt{x}$ is not hyperexponential but the sum of two hyperexponential functions. Its minimal order annihilating operator thus has order two and is the least common left multiple of two operators of order one. It is therefore not irreducible.

23. We have to show that $\theta(\Delta_i)$ is a K-linear combination of $\Delta_1, \ldots, \Delta_n$, for every i. Write $W(i_1, \ldots, i_s)$ for the determinant whose jth row is $\theta^{i_j}(y_0, \ldots, y_{s-1})$.

Case 1, $\sigma \neq \mathrm{id}$, $\delta = 0$: In this case, $\theta(W(i_1, \ldots, i_s)) = W(i_1 + 1, \ldots, i_s + 1)$. If $i_s + 1 < r$, then this is one of the Δ's. If $i_s + 1 = r$, we can use the operator to rewrite the last row $\theta^r(y_0, \ldots, y_{s-1})$ as a K-linear combination the rows $\theta^j(y_0, \ldots, y_{s-1})$

with $j < r$. Taking the linear combination out of the determinant, we obtain a K-linear combination of the Δ's.

Case 2, $\sigma = \mathrm{id}$, $\delta \neq 0$: Here, $\theta(W(i_1, \ldots, i_s)) = \sum_{j=1}^{s} W(i_1, \ldots, i_{j-1}, i_j + 1, i_{j+1}, \ldots, i_s)$, and each of the determinants in this sum is either zero or one of the Δ's or a determinant whose last row is $\theta^r(y_0, \ldots, y_{s-1})$ and can be handled like above. Altogether we again get a K-linear combination of the Δ's.

24. **a.** $(D^2-(x+1)D+x)(D^2+D-(x-3))$; **b.** $(D^3-D+x)(D^2+D-(x-1))$; **c.** $(S^2 - S + x)(S^2 + S - x)$; **d.** $(S^2 - (x+1)S + x)(S^2 + S - (x-3))$.

25. We found one isolated factor $D^2 - 1$ as well as the following three families of factors: $D^2+\frac{c_3x^2+(c_2-2c_3)x+c_1-c_2}{c_3x^2+c_2x+c_1}D-\frac{2c_3x+c_2}{c_3x^2+c_2x+c_1}$ for any choice $c_1, c_2, c_3 \in C$ with $(c_1, c_2, c_3) \neq (0, 0, 0)$; $D^2 - \frac{c_3x^2+(c_2+2c_3)x+c_1+c_2}{c_3x^2+c_2x+c_1}D + \frac{2c_3x+c_2}{c_3x^2+c_2x+c_1}$ for any choice $c_1, c_2, c_3 \in C$ with $(c_1, c_2, c_3) \neq (0, 0, 0)$; $D^2 - \frac{2c_3x+c_2}{c_3x^2+c_2x+c_1}D + \frac{2c_3}{c_3x^2+c_2x+c_1}$ for any choice $c_1, c_2, c_3 \in C$ with $(c_1, c_2, c_3) \neq (0, 0, 0)$.

26. If a family of factors can be found, the least common multiple M of several instances of the family will also be a right factor of L. Instead of taking only one factor P and proceeding recursively on $\mathrm{rquo}(L, P)$, we can proceed recursively on $\mathrm{rquo}(L, M)$ and $\mathrm{rquo}(M, P)$ and concatenate the resulting lists. Since the cost of factoring is very sensitive towards the order of the input operator, factoring the two smaller operators $\mathrm{rquo}(L, M)$ and $\mathrm{rquo}(M, P)$ is likely to be faster than factoring the one big operator $\mathrm{rquo}(L, P)$.

27. It is true that the vector space generated by all the $s \times s$ Wronskian-type determinants has the same dimension as the vector space generated by all the $(r - s) \times (r - s)$ Wronskian-type determinants, but note that the sizes of these determinants differ. By using adjoints, we can work with whatever the smaller of the two formats is.

28. Depending on the case, the commutation rule implies **a.** $(p\partial^{r/k} + \cdots)^k = (p\partial^{r/k})^k + \cdots = p^k\partial^r + \cdots$ and **b.** $(\cdots + p)^k = \cdots + p^k$.

29. Up to constant multiples, the unique hyperexponential solution of L is $x\sqrt{1-x}$. A factorization of L in $C(x)[D]$ is therefore $L = (\frac{2}{x}D + \frac{3}{x})((2x^2 - 2x)D + (2 - 3x))$. For a potential factorization $L = PQ$ with $P, Q \in C[x][D]$, we may have $\deg_D(P) = 0$, $\deg_D(Q) = 2$ or $\deg_D(P) = 1$, $\deg_D(Q) = 1$ or $\deg_D(P) = 2$, $\deg_D(Q) = 0$. The first case is impossible because the coefficients $4x-4$, $6x-4$, -9 are coprime. The last case is also impossible because we can write $L = D^2(4x-4)+D(6x-12)-15$ and $4x-4$, $6x-12$, -15 are coprime. Finally, the case $\deg_D(P) = 1$, $\deg_D(Q) = 1$ is also impossible, because any such factorization would have to be of the form $((\frac{2}{x}D+\frac{3}{x})q)(q^{-1}((2x^2-2x)D+(2-3x)))$ for some $q \in C(x)$ such that $(\frac{2}{x}D+\frac{3}{x})q$ and $q^{-1}((2x^2-2x)D+(2-3x))$ both are in $C[x][D]$. Because of the first factor, the numerator of q must be a multiple of x, but because of the second factor, the numerator of q cannot be a multiple of x. We have thus proved that there is no factorization of L in $C[x][D]$.

30. We have $L = (D^2 - D) \otimes (D^2 - 2D)$. This is relatively easy to find because L has constant coefficients, so it can be solved in terms of exponentials: $V(L)$ has $\{1, \exp(x), \exp(2x), \exp(3x)\}$ as a basis. Observing that $\exp(3x) = \exp(x)\exp(2x)$, and that $V(D^2-D)$ and $V(D^2-2D)$ are generated by $\{1, \exp(x)\}$ and $\{1, \exp(2x)\}$, respectively, we see that $V(L) \cong V(D^2 - D) \otimes V(D^2 - 2D)$.

For the case of non-constant coefficients, see [238, 407, 446, 448]; for the recurrence case, see [124, 126, 276].

Section 4.5

1. The reasoning of Example 4.64 shows that the dimension is at most 2. If the dimension were smaller, then $x + \exp(x + y)$ would satisfy a first order differential equation with respect to, say, x. But this means that $x + \exp(x + y)$ would be hyperexponential with respect to x, which is not the case, because x and $\exp(x + y)$ are not similar.

2. For x^n we have the annihilating operators $S_n - x$ and $xD_x - n$, so the intersection of $\operatorname{ann}(x^n)$ with any of $C(x, n)[D_x]$, $C(x, y)[S_n]$ is nonempty, so D-finiteness follows using Proposition 4.65.

If $\log(n + x)$ were D-finite, there would be an annihilating operator in $L \in C(x, n)[S_n]$. By multiplying the equation $L \cdot \log(n + x) = 0$ with a suitable element of $C(x, n)$ to clear denominators and common factors if necessary, we get an equation which does not vanish identically when x is set to zero. But this would mean that $\log(n)$ is D-finite, in contradiction to Exercise 8 from Sect. 2.4.

3. For every $\alpha \in \mathbb{Q}$, the annihilator is $\langle y(x + y)D_y - \alpha(2x + 3y), x(x + y)D_x - \alpha(4x + 3y)\rangle$. It cannot be smaller because the given generators evidently annihilate $(x^3(x + y)y^2)^\alpha$, and it cannot be larger because the ideal is maximal (since the quotient space has dimension 1), so any larger ideal will contain 1, which does not annihilate $(x^3(x + y)y^2)^\alpha$.

It is much more difficult to determine the annihilator in $C[x, y][D_x, D_y]$.

4. In this case there is nothing to show because 0 is clearly D-finite as well as holonomic.

5. By Theorem 4.69, holonomy with respect to $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$ is equivalent to D-finiteness with respect to $C(x_1, \dots, x_n)[D_{x_1}, \dots, D_{x_n}]$ and holonomy with respect to $C[x_1, \dots, x_n][\theta_{x_1}, \dots, \theta_{x_n}]$ is equivalent to D-finiteness w.r.t. $C(x_1, \dots, x_n)[\theta_{x_1}, \dots, \theta_{x_n}]$. Obviously, D-finiteness with respect to $C(x_1, \dots, x_n)[D_{x_1}, \dots, D_{x_n}]$ is equivalent to D-finiteness with respect to $C(x_1, \dots, x_n)[\theta_{x_1}, \dots, \theta_{x_n}]$. Consequently, holonomy with respect to $C[x_1, \dots, x_n][D_{x_1}, \dots, D_{x_n}]$ is equivalent to holonomy w.r.t. $C[x_1, \dots, x_n][\theta_{x_1}, \dots, \theta_{x_n}]$.

For the equivalence of holonomy of the sequence with respect to $C[k_1, \dots, k_n][S_{k_1}, \dots, S_{k_n}]$ and holonomy of its generating function with respect to $C[x_1,\ldots,x_n][\theta_{x_1},\ldots,\theta_{x_n}]$, note that an operator $L(k_1,\ldots,k_n,S_{k_1},\ldots,S_{k_n})$ annihilates a sequence if and only if the operator $L(\theta_{x_1},\ldots,\theta_{x_n},x_1^{-1},\ldots,x_n^{-1})$ annihilates the series. This implies that the defining property for holonomy is either satisfied for both or for neither of the two objects.

6. **a.** For every $u\in K$ and every $f\in F$ we have to show that $\partial_{n+1}\cdot uf=\partial_{n+1}u\cdot f$, which is evident since both sides are zero. **b.** By Proposition 4.65, we have to show that for every $i\in\{1,\ldots,n+1\}$ there is an annihilating operator of f in $K[\partial_i]\setminus\{0\}$. For $i\le n$, this is true because f is D-finite w.r.t. $K[\partial_1,\ldots,\partial_n]$, and for $i=n+1$, it is true because the action is defined in such a way that ∂_{n+1} is an annihilating operator.

7. False. A counterexample is given by the Stirling numbers of the second kind, which are not D-finite but for which we have the formula $S_2(n,k)=\frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$, which shows that they are D-finite with respect to n for every specific choice of k.

8. **a.** Let $c_1,\ldots,c_n\in C$ be such that $c_1r_1+\cdots+c_nr_n=0$ and let $i\in\{1,\ldots,n\}$ be arbitrary. We show that $c_i=0$. If $r_i=u/v$ for $u,v\in C[x]$ with $\gcd(u,v)=1$, then $c_1r_1v+\cdots+c_nr_nv=0$, and taking this modulo v gives $c_iu=0 \bmod v$, because the denominators of $r_1,\ldots,r_{i-1},r_{i+1},\ldots,r_n$ are coprime to v. Since u is also coprime to v, it follows that $c_i=0$. **b.** Let $u,v,u',v'\in\mathbb{Z}$ be such that $(u,v)\neq(u',v')$ and consider the polynomials $p=(m+u)^2+(x+v)^2$ and $p'=(m+u')^2+(x+v')^2$. These polynomials have a common factor if and only if their resultant is zero. We have $\operatorname{res}_x(p,p')=((u-u')^2+(v-v')^2)((2m+u+u')^2+(v-v')^2)$, and since $(u,v)\neq(u',v')$ and $m\notin\mathbb{Z}$, this cannot be zero.

9. True. Annihilating operators for $1/(n^2-k^2)$ include $(1+k-n)(1+k+n)S_k-(k-n)(k+n)$, $(k-1-n)(1+k+n)S_n-(k-n)(k+n)$, $(n+1)S_k^2S_n-(n+2)S_kS_n^2-nS_k+(n+1)S_n$, and $(k+1)S_n^2S_k-(k+2)S_nS_k^2-kS_n+(k+1)S_k$, so the intersection of $\operatorname{ann}(1/(n^2-k^2))$ with any of $C[n,k][S_k]$, $C[n,k][S_n]$, $C[n][S_n,S_k]$, $C[k][S_n,S_k]$ is not empty.

10. It is not. We show that there is no nonzero annihilating operator in $C[n][S_n,S_k]$. For every $i,j\in\mathbb{N}$ we have $S_n^iS_k^j\cdot\frac{1}{nk+1}=\frac{1}{nk+in+jk+ij+1}$, and we need to show that these are linearly independent over $C(n)$. Suppose that $c_1,\ldots,c_m\in C[n]$ are such that for certain pairwise distinct pairs $(i_1,j_1),\ldots,(i_m,j_m)$ we have $\frac{c_1}{nk+i_1n+j_1k+1}+\cdots+\frac{c_m}{nk+i_mn+j_mk+i_mj_m+1}=0$. For arbitrary $\ell\in\{1,\ldots,m\}$, multiplying this relation by $nk+i_\ell n+j_\ell k+i_\ell j_\ell+1$ and setting $k=-\frac{i_\ell n+i_\ell j_\ell+1}{n+j_\ell}$, we obtain $c_\ell=0$. Since ℓ was arbitrary, it follows that $c_1=\cdots=c_\ell=0$, as required. Note that none of the remaining denominators can vanish by setting $k=-\frac{i_\ell n+i_\ell j_\ell+1}{n+j_\ell}$ because (i_ℓ,j_ℓ) is distinct from all other pairs.

11. False. For example, take the ideals $I=\langle D_x-1\rangle$, $J=\langle(D_x-1)(D_x-2)\rangle$ of $C[x,D_x]$.

12. If it were, there would be an annihilating operator in $C(x,n)[D_x]$. Since

$$D_x^i \cdot \sum_{k=1}^{n} \frac{1}{x+k} = (-1)^i i! \sum_{k=1}^{n} \frac{1}{(x+k)^i}$$

for every i, this would mean that the sums $\sum_{k=1}^n \frac{1}{(x+k)^i}$ $(i = 1, 2, \dots)$ are linearly dependent over $C(x, n)$. But then the sums $\sum_{k=1}^n \frac{1}{k^i}$ $(i = 1, 2, \dots)$ would be linearly dependent over $C(n)$. Let $p_1, \dots, p_r \in C(n)$ be such that $\sum_{i=1}^r p_i(n) \sum_{k=1}^n \frac{1}{k^i} = 0$ for all n. By clearing denominators, we may assume $p_1, \dots, p_r \in C[n]$. Moreover, since $\sum_{k=1}^n \frac{1}{k} \sim \log(n)$ and $\sum_{k=1}^n \frac{1}{k^i}$ converges for $i \geq 2$, we may in fact assume that $p_1, \dots, p_r \in C$, and since $\sum_{k=1}^n \frac{1}{k^i} \in \mathbb{Q}$ for all n, i, we may furthermore assume that $p_1, \dots, p_r \in \mathbb{Q}$. Clearing again denominators, we may finally assume $p_1, \dots, p_r \in \mathbb{Z}$.

We have to show that $p_1 = \dots = p_r = 0$. Suppose otherwise and assume without loss of generality that $p_r \neq 0$ (otherwise replace r by a smaller number). Let $n \in \mathbb{N}$ be a prime that does not divide p_r. Then $n!^r \sum_{i=1}^r p_i \sum_{k=1}^n \frac{1}{k^i} = 0$ implies $(n-1)!^r p_r = -n!^r p_r \sum_{k=1}^{n-1} \frac{1}{k^i} - n!^r \sum_{i=1}^{r-1} p_i \sum_{k=1}^n \frac{1}{k^i}$. Both sides of this equation are integers, and the right hand side is a multiple of n while the left hand side is not. This is impossible.

13. Annihilating operators include $(x^2-1)D_x^2 + 2xD_x - n(n+1)$, $(n+2)S_n^2 - (2n+3)xS_n + (n+1)$, $D_x S_n^2 - 2xD_x S_n + D_x - S_n$, $D_x S_n^2 - D_x - (2n+3)S_n$, so the intersection of $\operatorname{ann}(P_n(x))$ with any of $C[n,x][D_x]$, $C[n,x][S_n]$, $C[x][D_x, S_n]$, $C[n][D_x, S_n]$ is not empty.

14. By the linear independence, there exist linear functions $h_1, \dots, h_m : \mathbb{Q}^n \to \mathbb{Q}$ such that $x_i = g_i(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$ for $i = 1, \dots, n$. Therefore, if $p \in \mathbb{Q}[y_1, \dots, y_m]$ is such that $p(g_1, \dots, g_m) = 0$, then setting y_j to $h_j(x_1, \dots, x_n)$ for $j = 1, \dots, m$ implies $p(x_1, \dots, x_n) = 0$, i.e., $p = 0$.

15. If a power series is D-finite, it is also holonomic (by Theorem 4.69), so its coefficient sequence is also holonomic (by Exercise 5). A holonomic sequence is in particular D-finite. Note however that the notion of D-finiteness is not directly applicable to sequences but only to germs of sequences. For example, the series $\sum_{n=0}^\infty x^n y^n$ is D-finite, and its coefficient sequence $(\delta_{n,k})_{n,k=0}^\infty$ is holonomic, but since this sequence is only nonzero when $n = k$, it is indistinguishable from the zero sequence as a germ. It is fair to say that the sequence is D-finite, although it may feel a bit disturbing that in this sense, every sequence $(a_n \delta_{n,k})_{n,k=0}^\infty$ is D-finite, even if $(a_n)_{n=0}^\infty$ is non-D-finite as a univariate sequence. Indeed, if $(a_n)_{n=0}^\infty$ is not D-finite, then in view of Exercise 26 the sequence $(a_n \delta_{n,k})_{n,k=0}^\infty$ is yet another example of a D-finite sequence whose generating function is not D-finite.

16. **a.** From $D_x - x, D_y - x \in \operatorname{ann}(f)$ it follows that $(D_y D_x - D_y x) - (D_x D_y - D_x x) = -D_y x + D_x x = -xD_y + xD_x + 1 \in \operatorname{ann}(f)$. It also follows that $x(D_x - x) - x(D_y - x) = xD_x - xD_y \in \operatorname{ann}(f)$, and from both together it follows that $1 \in \operatorname{ann}(f)$. This implies $f = 0$. **b.** Suppose that $\phi(f) = \binom{u}{v}$. We have to show that $u = v = 0$. From $\phi(D_x \cdot f) = A_x \binom{u}{v} + \binom{u_x}{v_x} = \binom{u+u_x}{-v+v_x}$ and $\phi(D_y \cdot f) = A_y \binom{u}{v} + \binom{u_y}{v_y} = \binom{v+u_y}{u+v_y}$ it follows

$$\phi(D_yD_x\cdot f)=A_y\begin{pmatrix}u+u_x\\-v+v_x\end{pmatrix}+\begin{pmatrix}u_y+u_{xy}\\-v_y+v_{xy}\end{pmatrix}=\begin{pmatrix}-v+v_x+u_y+u_{xy}\\u+u_x-v_y+v_{xy}\end{pmatrix},$$

$$\phi(D_xD_y\cdot f)=A_x\begin{pmatrix}v+u_y\\u+v_y\end{pmatrix}+\begin{pmatrix}v_x+u_{xy}\\u_x+v_{xy}\end{pmatrix}=\begin{pmatrix}v+u_y+v_x+u_{xy}\\-u-v_y+u_x+v_{xy}\end{pmatrix}.$$

Since both vectors must be equal, their difference $-2\binom{v}{u}$ is zero, so $u=v=0$.

17. Writing $A_i=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$ and $B_i=\begin{pmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{pmatrix}$, we can take

a. $A_i\otimes B_i=\begin{pmatrix}a_{11}b_{11}&a_{11}b_{12}&a_{12}b_{11}&a_{12}b_{12}\\a_{11}b_{21}&a_{11}b_{22}&a_{12}b_{11}&a_{12}b_{12}\\a_{21}b_{11}&a_{21}b_{12}&a_{22}b_{11}&a_{22}b_{12}\\a_{21}b_{21}&a_{21}b_{22}&a_{22}b_{11}&a_{22}b_{12}\end{pmatrix}$ or

b. $A_i\otimes I_2+I_2\otimes B_i=\begin{pmatrix}a_{1,1}+b_{1,1}&b_{1,2}&a_{1,2}&0\\b_{2,1}&a_{1,1}+b_{2,2}&0&a_{1,2}\\b_{2,1}&0&a_{2,2}+b_{1,1}&b_{1,2}\\0&b_{2,1}&b_{2,1}&a_{2,2}+b_{2,2}\end{pmatrix}$,

respectively.

18. First Theorem 4.72 part 1 applied to f shows that $f(n,k,\sqrt{1-xy},x^2+y^2)$ is D-finite, then Theorem 4.72 part 2 applied to this function shows that $f(3n+5,2n-k,\sqrt{1-xy},x^2+y^2)$ is D-finite.

19. Write $v=(v_1,\dots,v_n)$. We may assume that the components of v are integers (otherwise stretch v appropriately) and that v is nonzero (otherwise f is constant and thus holonomic). For any $i,j\in\{1,\dots,n\}$ with $i\neq j$, we have $S_{k_i}^{\max(0,-v_j)}S_{k_j}^{\max(0,-v_i)}(S_{k_i}^{v_j}-S_{k_j}^{v_i})\cdot f=0$, so for every variable set containing at least two shift operators, there is a nontrivial annihilating operator involving this variable set. The remaining variable sets to be considered consist of one shift operator S_{k_i} and all the variables $k_1,\dots,k_n$. For any $i\in\{1,\dots,n\}$, note that $(S_{k_i}-1)\cdot f$ is zero for all points $(k_1,\dots,k_n)$ which are not on the boundary of the halfspace defined by u and v. Therefore, $\big(((k_1,\dots,k_n)-u)\cdot v\big)(S_{k_i}-1)$ is a nonzero annihilating operator of f involving only $k_1,\dots,k_n$ and S_{k_i}.

20. A basis of $C(x,y)[D_x,D_y]/I$ is $\{[1],[D_y]\}$, and we can define ϕ by $\phi([u+vD_y])=\binom{u}{v}$. Then the actions of D_x,D_y on vectors are given by the companion matrices $\begin{pmatrix}-y/(xy-1)&-(1+xy)/(xy-1)\\y^2/(xy-1)&y(1+xy)/(xy-1)\end{pmatrix}$ and $\begin{pmatrix}0&-x^2/(xy-1)\\1&x^2y/(xy-1)\end{pmatrix}$, respectively.

21. Algorithm 4.73 gives $I=\langle(-k^2-3n^2-4n-1)S_k+(2k+1)(k-n-1)S_n-(k-3n-2)(k+n+1),\ (2k+1)(k+n+2)S_k^2-2(k+1)(2n+1)S_k-(2k+3)(k-n)\rangle$ or possibly a different basis for the same ideal, depending on the chosen term order. We cannot conclude that $I=\operatorname{ann}(f)$ without additional knowledge of f. It could be, for example, that f is constant, and then $I\subsetneq\operatorname{ann}(f)=\langle S_n-1,S_k-1\rangle$.

22. With the help of Algorithm 4.73 we can find that the ideal $I = \langle -(x-1)^2(x+1)^2D_x^3 - 6(x-1)x(x+1)D_x^2 + 2(2n^2x^2 - 2n^2 + 2nx^2 - 2n - 3x^2 + 1)D_x + 4n(n+1)x, 2(n+1)^2S_n - 2(n+2)(x-1)x(x+1)D_x - (x-1)^2(x+1)^2D_x^2 - 2(n+1)(n+x^2)\rangle \subseteq C(n,x)[S_n, D_x]$ is contained in $\operatorname{ann}(P_n(x)^2)$, but it remains to check that the ideals are equal. We also know from Algorithm 4.73 that $\dim_{C(n,x)} C(n,x)[S_n, D_x]/I = 3$, and that $\{[1], [D_x], [D_x^2]\}$ is a basis. Therefore, the only way $\operatorname{ann}(P_n(x)^2)$ could be larger than I is that $P_n(x)^2$ satisfies a linear differential equation with coefficients in $C(n,x)$ of order less than three. The minimal order operator annihilating $P_n(x)^2$ must be a right factor of any operator of $I \cap C(n,x)[D_x]$. The first generator in the ideal basis above is a third order operator in D_x, for which we can check with the algorithms of the previous section that it is irreducible. This shows that $\operatorname{ann}(P_n(x)^2) = I$.

23. $I = \langle 2xD_x + 4yD_y - 1, 4y(x^2 - 4y)D_y^2 + 2(x^2 - 8y)D_y + 1\rangle$.

24. If $(a_{n,k})_{n,k=0}^\infty$, $(b_{n,k})_{n,k=0}^\infty$ are holonomic sequences, then $a(x,y) = \sum_{n,k=0}^\infty a_{n,k}x^ny^k$ and $b(x,y) = \sum_{n,k=0}^\infty b_{n,k}x^ny^k$ are holonomic series. By Theorem 4.69, these series are then also D-finite. Since D-finiteness is preserved by addition, the series $c(x,y) := \sum_{n,k=0}^\infty (a_{n,k} + b_{n,k})x^ny^k$ is D-finite, hence also holonomic. It finally follows that $(a_{n,k} + b_{n,k})_{n,k=0}^\infty$ is holonomic.

25. **a.** Since $a(x,y)$ is D-finite, there is at least some nonzero annihilating operator $L(x,y,D_x)$ of $a(x,y)$. Exchanging x and y in the equation $L(x,y,D_y)\cdot a(x,y) = 0$ gives $L(y,x,D_y)\cdot a(y,x) = 0$, and since $a(x,y) = a(y,x)$ by assumption, we find that $L(y,x,D_y)$ is a nonzero annihilating operator as well. Therefore $L(x,y,D_x) + L(y,x,D_y)$ is an annihilating operator for $a(x,y)$. This operator is symmetric, and it is nonzero because $L(x,y,D_x)$ must involve D_x if $a(x,y)$ is not the zero series. **b.** If L is a symmetric annihilating operator, D_xL is an asymmetric annihilating operator.

26. **a.** If $u(x,y) := a(xy)$ is D-finite, so is $u(x, y/x) = a(x)$ by part 1 of Theorem 4.72. This means $a(x)$ is D-finite with respect to $C(x,y)[D_x, D_y]$. Its annihilator contains a nonzero element of $C(x,y)[D_x]$, say $L = \sum_{i=0}^d y^iL_i(x,D_x)$ for certain $L_i(x,D_x) \in C(x)[D_x]$. Since $a(x)$ is free of y, it must already be annihilated by each $L_i(x,D_x)$, and since at least one of them is nonzero, we have found an annihilating operator of a in $C(x)[D_x]$, so a is D-finite in the univariate sense. **b.** Writing $a = \sum_{n,k=0}^\infty a_{n,k}x^ny^k$, the annihilating operator $(xD_x - yD_y)^s$ of a translates into a recurrence operator $(n-k)^s\cdot(a_{n,k})_{n,k=0}^\infty = 0$, which implies that $a_{n,k} = 0$ whenever $n \neq k$. The claim follows.

27. We show that if we have an algorithm for deciding the existence of polynomial solutions of given linear operators then there is also an algorithm for deciding the existence of integer roots of polynomials with integer coefficients.

Suppose we are given a polynomial $p \in \mathbb{Z}^n$ and have to decide whether it admits a root $(\xi_1, \ldots, \xi_n) \in \mathbb{N}^n$. If we write p in the form $p = \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n}x_1^{\underline{i_1}}\cdots x_n^{\underline{i_n}}$ and consider the operator

$$L = \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} D_{x_1}^{i_1} \cdots D_{x_n}^{i_n},$$

then for every $(\xi_1, \ldots, \xi_n) \in \mathbb{N}^n$ we have $L \cdot x_1^{\xi_1} \cdots x_n^{\xi_n} = p(\xi_1, \ldots, \xi_n) x_1^{\xi_1} \cdots x_n^{\xi_n}$. Since the terms $x_1^{\xi_1} \cdots x_n^{\xi_n}$ are linearly independent over C, it follows that a nonzero polynomial solution of L exists if and only if p has a root in $\mathbb{N}^r$. Therefore, if there were an algorithm for deciding the existence of polynomial solutions, there would be an algorithm for finding integer roots.

It is also not decidable whether a differential or difference operator has rational function solutions [348], although it is possible to derive certain constraints on the possible denominators of rational function solutions [272, 273].

Section 4.6

1. "⇒": $I = \bigcup_{m=1}^{\infty} I_m$ is an ideal of $K[X_1, \ldots, X_n]$, and by assumption it has a finite basis $\{b_1, \ldots, b_k\}$. Each element of this basis belongs to a certain I_m, and because of the mutual inclusions, there is an m such that $b_1, \ldots, b_k$ all belong to I_m. For this m we have $I_m = I_{m+1} = \cdots = I$.

"⇐": Let $I \in K[X_1, \ldots, X_n]$ be an ideal. If I is not finitely generated, then there exist $p_1, p_2, \cdots \in I$ such that $p_m \notin \langle p_1, \ldots, p_{m-1} \rangle$ for all m, so setting $I_m = \langle p_1, \ldots, p_m \rangle$ gives a non-stabilizing chain $I_1 \subsetneq I_2 \subsetneq \cdots$, which is in conflict with the assumption.

2. Since the ∂_i commute with each other (though not necessarily with elements of K), all requirements carry over directly.

3. The commutation rules $D_i x_i = x_i D_i + 1$ and $S_i x_i = x_i S_i + S_i$ meet requirement (iii), because if $\leq$ is a term order for the commutative case, then $1 \leq x_i D_i$ and $S_i \leq x_i S_i$ are guaranteed. Since (iii) holds, we know that $\operatorname{lt}(\rho\tau)$ is the term obtained from $\rho\tau$ by sorting the variables. Therefore (ii) follows from the assumption that $\leq$ is a term order for the commutative case. It is also clear that (i) holds.

4. The commutation rule is in conflict with condition (iii) in the definition of term orders.

5. For the algebra from the previous exercise, the lexicographic order with $x > M$ satisfies (i) and (ii) but not (iii).

6. Replace line 1 by "$r = 0$, $q_1 = \cdots = q_m = 0$" and line 8 by "return $r, q_1, \ldots, q_m$", and add the following after line 5: "5a for an i with $g = g_i$, set $q_i = q_i + ([\tau]p)\sigma \operatorname{lc}(g)^{-1}$".

7. Without loss of generality, we may assume $\operatorname{lc}(g) = 1$ for all $g \in G$. Let d be the coefficient of $\operatorname{lt}(\tau g)$ in p. We distinguish three cases. (i) $d = 0$. In this case, the monomial $c \operatorname{lm}(\tau g)$ appears in $p + c\tau g$. With one reduction step, we can get from $p + c\tau g$ to p, and with zero or more additional reduction steps, we can get from there to $\operatorname{red}(p, G)$. Since remainders are assumed to be unique, we must have $\operatorname{red}(p + c\tau g, G) = \operatorname{red}(p, G)$. (ii) $d \neq 0$ and $d + c = 0$. In this case, the monomial $d\operatorname{lm}(\tau g)$ appears in p, and with one reduction step, we can get to $p + c\tau g$. From here, we get with zero or more additional reduction steps to $\operatorname{red}(p + c\tau g, G)$. Since remainders are assumed to be unique, we must have $\operatorname{red}(p + c\tau g, G) = \operatorname{red}(p, G)$. (iii) $d \neq 0$ and $d + c \neq 0$. In this case, we can get in one reduction step from p to $q = p - d\tau g$, which does not contain the term $\operatorname{lt}(\tau g)$. Since $d + c \neq 0$, we can also get in one reduction step from $p + c\tau g$ to q. Since remainders are assumed to be unique, we must have $\operatorname{red}(p, G) = \operatorname{red}(q, G) = \operatorname{red}(p + c\tau g, G)$.

8. $\{(4y + 1)D_y^2 + (-8y - 6)D_y + (-12y - 7), D_x D_y + D_x - D_y - 1, (4y + 1)D_x^2 + (-16y - 4)D_x - yD_y + (15y + 4)\}$.

9. "$\Rightarrow$": Suppose on the contrary that there is some i for which there is no $g \in G$ such that $\operatorname{lt}(g)$ is a power of X_i. Then none of the powers X_i can be reduced, so the classes $[1], [X_i], [X_i^2], \ldots$ are all linearly independent over K. Therefore $\dim_K K[X_1, \ldots, X_n]/I = \infty$.

"$\Leftarrow$": If $e_1, \ldots, e_n \in \mathbb{N}$ are such that $X_1^{e_1}, \ldots, X_n^{e_n}$ are leading terms of certain elements of G, then a term $X_1^{u_1} \ldots X_n^{u_n}$ is reducible as soon as $u_i \geq e_i$ for some i. Hence for all irreducible terms we must have $0 \leq u_i \leq e_i$ for all i, so their number is bounded by the product $e_1 e_2 \cdots e_n$, which is finite. By condition 4 of Theorem 4.77, it follows that $\dim_K K[X_1, \ldots, X_n]/I$ is finite.

10. "$\Rightarrow$": Since G is a Gröbner basis and $1 \in \langle G \rangle = I$, we must have $\operatorname{red}(1, G) = 0$. Therefore, G must contain an element g whose leading term is 1. Since 1 is the smallest term in the term order, g cannot have any further terms, so g is of the required form. "$\Leftarrow$": $u \in I \Rightarrow u^{-1}u = 1 \in I$.

11. Regardless of the term order, the equivalence classes of the terms in question form a K-vector space basis of $K[X_1, \ldots, X_n]/I$, so their number must be equal to the dimension of this space. The sets of terms may be different though. For example, in the commutative case, $I = \langle xy - 1, x^3 - 1 \rangle \subseteq C[x, y]$ has the Gröbner basis $G_1 = \{y^3 + 1, x + y^2\}$ with respect to the lexicographic term order with $x > y$, and the Gröbner basis $G_2 = \{y^2 + x, xy - 1, x^2 + y\}$ with respect to a degree order. The irreducible terms are $1, y, y^2$ in the first case and $1, x, y$ in the second case.

12. Although the term order is not specified, it is clear that only S_n and S_k can be the leading terms of the given generators. For the first example, the only S-polynomial is $\frac{n+1}{n-k}S_k - \frac{2(k-n-1)}{k+1}S_n$. It can be reduced with the first generator to $\frac{n+1}{n-k}S_k - \frac{2(n+1)}{k+1}$, which in turn can be reduced with the second generator to zero. Since there are no further S-polynomials, we have a Gröbner basis. For the second example, the only S-polynomial is $\frac{n+1}{n-k}S_k - \frac{2(k+n+1)}{k+1}S_n$. It can be reduced with the first generator to $\frac{n+1}{n-k}S_k - \frac{2(n+1)(k+n+1)}{(k+1)(k-n-1)}$, which in turn can be reduced with the second generator to $\frac{4k(n+1)}{(k+1)(k-n-1)(k-n)} \neq 0$. Since this cannot be reduced further, we do not have a Gröbner basis.

13. For every p we have $\operatorname{spol}(p, p) = 0$, so all pairs of the form (p, p) reduce to zero automatically and therefore need not be considered. Moreover, for all p, q we have $\operatorname{spol}(p, q) = -\operatorname{spol}(q, p)$, so whenever we arrange that $\operatorname{spol}(p, q)$ reduces to zero, then also $\operatorname{spol}(q, p)$ reduces to zero, so we need not also handle this pair.

14. A Gröbner basis of I is $\{2x(xy+1)D_x - (2y+1)(xy+x+1)D_y, -(xy+1)(xy+x-1)D_y^2 - x(2xy-x+4)D_y\}$. The leading terms are D_x and D_y^2, so by the result of Exercise 9, $C(x, y)[D_x, D_y]/I$ has finite dimension.

15. From the given generators we already see that $I \cap C[n, k][S_n]$ and $I \cap C[n, k][S_k]$ are not $\{0\}$. It remains to show that $I \cap C[n][S_n, S_k]$ and $I \cap C[k][S_n, S_k]$ are not $\{0\}$. This can be done by computing Gröbner bases of I with respect to orders that eliminate k or n, respectively.

16. For example, take $p = D_x + y, q = D_y \in C(x, y)[D_x, D_y]$. We have $\operatorname{lexp}(p) = (1, 0)$, $\operatorname{lexp}(q) = (0, 1)$, so $\min(\operatorname{lexp}(p), \operatorname{lexp}(q)) = (0, 0)$. However, $\operatorname{spol}(p, q) = D_y p - D_x q = D_y y = yD_y + 1$ and $\operatorname{red}(yD_y + 1, \{p, q\}) = 1 \neq 0$.

17. We have

$$\begin{aligned}
\operatorname{spol}(u, v) &= X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(u)} \operatorname{lc}(u)^{-1} u \\
&\quad - X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(v)} \operatorname{lc}(v)^{-1} v \\
&= X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(u)} \operatorname{lc}(u)^{-1} u \\
&\quad - X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(p)} \operatorname{lc}(p)^{-1} p \\
&\quad + X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(p)} \operatorname{lc}(p)^{-1} p \\
&\quad - X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\operatorname{lexp}(v)} \operatorname{lc}(v)^{-1} v \\
&= X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\max(\operatorname{lexp}(u),\operatorname{lexp}(p))} \operatorname{spol}(u, p) \\
&\quad + X^{\max(\operatorname{lexp}(u),\operatorname{lexp}(v))-\max(\operatorname{lexp}(p),\operatorname{lexp}(v))} \operatorname{spol}(p, v).
\end{aligned}$$

Plugging in the assumed representations of $\operatorname{spol}(u, p)$ and $\operatorname{spol}(p, v)$ gives a representation of the required form.

Thanks to the property proved here, it is possible to delete a pair (u, v) from P whenever there is a p with $(u, p), (p, v) \in P$ and $\operatorname{lexp}(p) \leq \max(\operatorname{lexp}(u), \operatorname{lexp}(v))$.

18. The assumption $\operatorname{lexp}(g) \leq \operatorname{lexp}(h)$ implies that whenever an element can be reduced with h it can also be reduced with g. Therefore, for every $p \in K[X_1, \ldots, X_n]$ we have $\operatorname{red}(p, G) = \operatorname{red}(p, G \setminus \{h\})$. The claim follows.

19. The given generators form a Gröbner basis G. In order to find the required element, we compute the remainders $\operatorname{red}((S_n D_x)^i, G)$ for $i = 0, 1, 2, \ldots$. Since they are all $C(n, x)$-linear combinations of $1, S_n, D_x$, the first four of them are linearly dependent. The linear dependence is the desired operator. It turns out to be $(x-1)(x+1)(D_x S_n)^3 - (2nx^2 - 2n + 5x^2 - 9)(D_x S_n)^2 - (n+3)(n+4)(D_x S_n)$.

20. Yes, if the new variable t commutes with all other variables. "$\subseteq$": if $p \in I \cap J$, then $(t + (1 - t))p = tp + (1 - t)p \in tI + (1 - t)J$. "$\supseteq$": if $p \in (tI+(1-t)J) \cap K[X_1, \dots, X_n]$, then p is a $K[t, X_1, \dots, X_n]$-linear combination of tb_i $(i = 1, \dots, m)$ and $(1-t)d_j$ $(j = 1, \dots, k)$. Setting $t = 0$ in this representation shows $p \in J$, and setting $t = 1$ shows $p \in I$. Note that p is free of t so it is not affected by setting t to 0 or 1.

Section 5.1

1. From $\gcd(u, v) = \gcd(v', v) = 1$ follows $\gcd(uv', v) = 1$, and by the extended Euclidean algorithm there are (and we can find) $s, t \in C[x]$ such that $suv' + tv = 1$, i.e., $suv' \equiv 1 \bmod v$. Therefore $b = -sa/(m - 1)$ is a solution. If there are two solutions $b, \tilde{b}$ of degree less than $\deg(v)$, then taking the difference of $a \equiv -(m - 1)buv' \bmod v$ and $a \equiv -(m - 1)\tilde{b}uv' \bmod v$, multiplying by s and dividing by $-(m - 1)$ gives $0 \equiv (b - \tilde{b}) \bmod v$, so $b = \tilde{b}$.

2. a. Hermite's algorithm finds a pair (g, h) of rational functions whose numerators have lower degree than the corresponding denominators, so if we choose $n = -1 + \sum_{i=1}^{m}(i - 1) \deg d_i$ and $k = -1 + \sum_{i=1}^{m} \deg d_i$, we can be sure to find at least one solution. **b.** Yes. If there are two pairs (g_1, h_1) and (g_2, h_2) then $(g_1-g_2)' = h_2-h_1$ shows that h_2-h_1 admits a rational integral. On the other hand, the denominator of $h_2 - h_1$ is squarefree, and the only way out is that $h_2 - h_1 = 0$, i.e., $h_1 = h_2$. This in turn implies that $g_1 - g_2$ is constant, but since $g_1 - g_2$ is at the same time a rational function whose numerator has lower degree than its denominator, it follows that $g_1 - g_2 = 0$, so $g_1 = g_2$. **c.** Using the degree bounds of part a for the ansatz, we get a linear system with $\deg d$ variables and at most $\deg d$ equations. The solution of a system can be found with $\mathrm{O}((\deg d)^{\omega})$ operations in C.

3. a. By $\gcd(p, q) = 1$, the Sylvester matrix for p and q is invertible. Therefore, there exist unique $s, t \in C[x]$ with $\deg s < \deg p$ and $\deg t < \deg q$ and $sq + tp = u$. The equation $sq+tp = u$ is equivalent to $s/p+t/q = u/(pq)$. **b.** For $t = \mathrm{quo}(u, p)$ and $s = \mathrm{rem}(u, p)$ we have $\frac{u}{p^n} = \frac{tp+s}{p^n} = \frac{s}{p^n} + \frac{t}{p^{n-1}}$ and $\deg s < \deg p$ and $\deg t < (n - 1) \deg p$. This shows the existence. For the uniqueness, observe that $\frac{u}{p^n} = \frac{s}{p^n} + \frac{t}{p^{n-1}}$ implies $u = tp + s$, which together with the imposed degree bounds and the uniqueness of quotient and remainder implies $t = \mathrm{quo}(u, p)$ and $s = \mathrm{rem}(u, p)$.

4. a. By Theorem 5.4, the formula holds when q is squarefree, but it does not hold when q is not squarefree. In fact, it does not even make sense in this case, because then $q'(\alpha) = 0$ for every root α of q. **b.** False. For example, $\mathrm{Res}_{x-\alpha}x^{-2} = 0$ for all $\alpha \in \bar{C}$. **c.** True. This follows directly from the existence and uniqueness of partial fraction decompositions.

5. a. No. $\mathrm{res}_x(q, p - zq') \in C[z]$ has zero as a root if and only if $\mathrm{res}_x(q, p) = 0$, which is equivalent to $\gcd(p, q) \neq 1$ and excluded by assumption. **b.** Yes. For example, for $q = x(x-1)$ and $p = q' = 2x-1$ we have $\operatorname{res}(q, p-zq') = -(1+z)^2$. **c.** No. Since $\deg(q) > 0$, there is an $\alpha \in \bar{C}$ which is a root of q, and since q is squarefree, α will not also be a root of q'. Therefore, for the choice $z = p(\alpha)/q'(\alpha)$ we have that α is a root of $p - zq'$, and thus a common root of q and $p - zq'$. Then $\gcd(q, p-zq') \neq 1$ implies $\operatorname{res}_x(q, p-zq') = 0$, so this z is a root of the resultant. **d.** No, because otherwise it will have zero as a root, which is excluded by part a.

6. **a.** $\frac{5x^2+3}{x^2(x+1)} + \log(x) + \frac{1}{2}\log(x+1)$; **b.** $\frac{1}{1-2x^2} + \sqrt{2}\log(1-\sqrt{2}x) - \sqrt{2}\log(\sqrt{2}x+1)$; **c.** $-\frac{5}{x^4} + \frac{3}{x^3} - \frac{1}{x^2} - \frac{2}{x} + 7\log(x)$; **d.** $\frac{9x^2-32x+27}{4(x-2)^2(x-1)} + \frac{17}{8}\log(x-2) - 2\log(x-1) - \frac{1}{8}\log(x)$.

7. The falling factorials $x^{\underline{n}} = x(x-1)\cdots(x-n+1)$ $(n \in \mathbb{N})$ form a C-vector space basis of $C[x]$. The claim follows from the observation that for every $n \in \mathbb{N}$ the equation $g(x+1) - g(x) = x^{\underline{n}}$ has the solution $g(x) = \frac{1}{n+1}x^{\underline{n+1}}$.

8. **a.** Let $g = \frac{p}{q}$ with $\gcd(p, q) = 1$ and let $h \in C[x]$ be an irreducible factor of q such that $\sigma^{-n}(h) \nmid q$ for all $n > 1$. Furthermore, let $m \in \mathbb{N}$ be maximal such that $\sigma^m(h) \mid q$. Then h and $\sigma^{m+1}(h)$ both divide the denominator of $\Delta g = \sigma(\frac{p}{q}) - \frac{p}{q} = \frac{\sigma(p)q - p\sigma(q)}{q\sigma(q)}$. Indeed, if we had $h \mid \sigma(p)q - p\sigma(q)$, then $h \mid \sigma(q)$, because $h \mid q$ and $h \nmid p$. But then $\sigma^{-1}(h) \mid q$, which is excluded. Similarly, if we had $\sigma^{m+1}(h) \mid \sigma(p)q - p\sigma(q)$, then $\sigma^{m+1}(h) \mid q$, because $\sigma^{m+1}(h) \mid \sigma(q)$ and $\sigma^{m+1}(h) \nmid \sigma(p)$, which is excluded by the choice of m. So the factors h and $\sigma^{m+1}(h)$ of the denominator $q\sigma(q)$ have no chance to be canceled by the numerator. **b.** If u is a common divisor of v and $\sigma^{m-1}(v)$, then $\sigma^{-(m-1)}(u)$ divides v, and therefore d, and $\sigma^{m-1}(u)$ divides $\sigma^{m-1}(v)$, and therefore d. This contradicts the assumed maximality of m. **c.** Let $v = \gcd(d, \sigma^{-(m-1)}(d))$ so that $v \mid d$ and $\sigma^{m-1}(v) \mid d$. By assumption on m, we have $\deg(v) > 0$. Set $q = \sigma^{\overline{m}}(v)/\gcd(\sigma^{\overline{m}}(v), d)$ and define $\tilde{a} = aq$, $\tilde{d} = dq$, so that $f = a/d = \tilde{a}/\tilde{d}$ and $\sigma^{\overline{m}}(v) \mid \tilde{d}$, then set $u = \tilde{d}/\sigma^{\overline{m}}(v)$ to get $f = \frac{\tilde{a}}{u\sigma^{\overline{m}}(v)}$. If we do not have $\gcd(u, v) = 1$, repeat the construction with $v\gcd(u, v)$ in place of v. **d.** Using $\Delta\frac{b}{\sigma^{\overline{m-1}}(v)} = \frac{\sigma(b)v - b\sigma^{m-1}(v)}{\sigma^{\overline{m}}(v)}$ and multiplying the desired equation by $u\sigma^{\overline{m}}(v)$ gives $\tilde{a} = u\sigma(b)v - ub\sigma^{m-1}(v) + cv$. Taking this equation modulo v gives $\tilde{a} \equiv -u\sigma^{m-1}(v)b \bmod v$, which by the assumption $\gcd(u, v) = \gcd(\sigma^{m-1}(v), v) = 1$ can be solved for a $b \in C[x]$ with $\deg b < \deg v$. Knowing b, we can compute $c = (\tilde{a} - u\sigma(b)v + ub\sigma^{m-1}(v))/v$. For a more detailed discussion of Hermite reduction in the summation case, see [349]. In particular, this paper contains an appropriate analog of the squarefree decomposition of d. **e.** $\frac{(n+1)(3n+8)}{4(n+2)(n+3)}$

9. **a.** $(x^2+4x-3)\exp(x^3+x^2+x)$; **b.** $\frac{x+2}{1-x}\exp\left(\frac{x^2}{x-1}\right)$; **c.** $(1+\frac{1}{x})^{\sqrt{2}}x(x+1)\exp(x)$; **d.** $\frac{2}{3}\sqrt{x^2+x+1}(8x^2-10x-1)$.

10. For $f(x) = \exp(-x^2)$ we have $f'(x)/f(x) = -2x = q/r + p'/p$ for $q = -2x$ and $p = r = 1$. The Gosper equation $y' + 2xy = 1$ has no polynomial solution, because $\deg(2xy) > \deg(y) > \deg(1-y')$ is in contradiction to $2xy = 1 - y'$. The claim follows.

11. Regardless of the choice of $h_i(x)$, the derivative $\big(\gamma_i \log(h_i(x))\big)' = \gamma_i h_i'(x)/h_i(x)$ will always be a rational function. Therefore, $\big(\sum_{i=1}^k \gamma_i \log(h_i(x))\big)'$ is a rational function. In order for the sum of a rational function with $g(x)$ to be hyperexponential, $g(x)$ must also be rational, because the sum of two dissimilar hyperexponential functions is not hyperexponential. It follows that if there is a closed form of the format in question with $k \geq 1$ but none with $k = 0$, the integrand $f(x)$ must be rational.

12. The direction "$\Leftarrow$" is true: using integration by parts and induction on the degree of p, it is easy to see that each such term is integrable, and that the integral is again an expression of the same form. The direction "$\Rightarrow$" is false: for example, also $x^{1/2}$ can be integrated arbitrarily often but is not of the form under consideration. Functions that can be integrated arbitrarily often were studied by Chen [127].

13. If f denotes the integrand, then $\frac{f'}{f} = \frac{2\alpha x+2\alpha+2x^2+3x}{2x(\alpha+x)}$. Taking $q = 2x+2\alpha+1$, $r = 2(x+\alpha)$, and $p = x$, we have $\frac{f'}{f} = \frac{q}{r} + \frac{p'}{p}$ and $\gcd(r, q - ir') = \gcd(x + \alpha, x + \alpha + \frac{1}{2} - i) = 1$ for all $i \in \mathbb{N}$, so we have a Gosper form of f'/f. The Gosper equation is $2(\alpha + x)y' + (2x + 2\alpha + 3)y = x$. The indicial polynomial for this equation is $\eta = 2$, so any solution y can have degree at most zero. Then $y' = 0$ and the equation simplifies to $2xy + (2\alpha + 3)y = x$, which forces $y = 1/2$ and $\alpha = -3/2$.

14. If h^i and h^j were similar, then h^{i-j} would be rational, in contradiction to the assumption that h is transcendental. Any $f \in R$ has the form $f = f_0 + f_1 h + \cdots + f_d h^d$ for certain $f_0, \ldots, f_d \in C(x)$. As powers of h are pairwise non-similar, an integral g, if it exists, must be of the form $g = g_0 + \cdots + g_d h^d$ for certain $g_0, \ldots, g_d \in C(x)$, and in fact, we must have $(g_i h^i)' = f_i h^i$ for each i. Whether such $g_0, \ldots, g_d$ exist can therefore be decided by the Almkvist-Zeilberger algorithm.

15. For a $g = g_0 + \cdots + g_d \log(x)^d \in C(x)[\log(x)]$ with $g_d \neq 0$, we have $g' = g_0' + \cdots + g_d' \log(x)^d + d g_d \log(x)^{d-1}/x = (g_0' + g_1/x) + \cdots + (g_{d-1}' + d g_d/x) \log(x)^{d-1} + g_d' \log(x)^d$. Unless g_d is a nonzero constant, the degree of g in $\log(x)$ is again d. If g_d is a nonzero constant, then $g_{d-1}' + d g_d/x$ is nonzero, because $1/x$ is not integrable in $C(x)$, therefore the degree of g in $\log(x)$ is $d - 1$ in this case. Given $f = f_0 + \cdots + f_d \log(x)^d \in C(x)[\log(x)]$ with $f_d \neq 0$, an integral g in $C(x)[\log(x)]$, if it exists, must therefore be of the form $g = g_0 + \cdots + g_{d+1} \log(x)^{d+1}$ for certain $g_0, \ldots, g_{d+1} \in C(x)$. Equating coefficients of powers of $\log(x)$ in $g' - f$ to zero gives a first order coupled linear differential system for $g_0, \ldots, g_{d+1}$, which can be solved with the techniques of Sect. 4.3.

16. We describe an algorithm for computing such a decomposition. Start with $q = u$, $r = v$, $p = 1$. If $\gcd(r, q - ir') = 1$ for all $i \in \mathbb{N}$, we are done. Otherwise, let i be maximal such that $g := \gcd(r, q - ir') \neq 1$ and set $p_{\mathrm{new}} = g^i p$, $r_{\mathrm{new}} = r/g$, and $q_{\mathrm{new}} = (q - i r_{\mathrm{new}} g')/g$. Note that $g \mid q - ir' = q - i(r_{\mathrm{new}} g)' = q - i r_{\mathrm{new}} g' - i r_{\mathrm{new}}' g$ implies $g \mid q - i r_{\mathrm{new}} g'$, so both r_{new} and q_{new} are polynomials. Moreover,

$$\frac{q_{\text{new}}}{r_{\text{new}}} + \frac{p'_{\text{new}}}{p_{\text{new}}} = \frac{(q - ir_{\text{new}}g')/g}{r_{\text{new}}} + \frac{(g^i p)'}{g^i p} = \frac{q}{r} - i\frac{g'}{g} + i\frac{g'}{g} + \frac{p'}{p} = \frac{u}{v}.$$

If we now have $\gcd(r_{\text{new}}, q_{\text{new}} - ir'_{\text{new}}) = 1$ for all $i \in \mathbb{N}$, then we are done. Otherwise, repeat the procedure with $p_{\text{new}}, q_{\text{new}}, r_{\text{new}}$ in place of p, q, r. Since $\deg r$ becomes strictly smaller in each iteration, we must come to an end after finitely many repetitions.

17. a. $\frac{g'}{g} = \frac{(uf)'}{uf} = \frac{u'f+uf'}{uf} = \frac{u'}{u} + \frac{f'}{f} = \frac{q}{r} + \frac{p'}{p} + \frac{u'}{u} = \frac{(up)'}{up}$, and it is clear that the requirement $\gcd(r, q - ir') = 1$ $(i \in \mathbb{N})$, which does not depend on p, is not affected. **b.** $\frac{\sigma(g)}{g} = \frac{\sigma(u)}{u}\frac{\sigma(f)}{f} = \frac{\sigma(u)}{u}\frac{\sigma(p)q}{p\sigma(r)} = \frac{\sigma(up)q}{(up)\sigma(r)}$, and it is clear that the requirement $\gcd(q, \sigma^i(r)) = 1$ $(i \in \mathbb{N})$, which does not depend on p, is not affected.

18. It is easy to confirm by a calculation that we indeed have $\frac{qt-rt'}{rt} + \frac{(pt)'}{pt} = \frac{q}{r} + \frac{p'}{p}$. It remains to show that $\gcd(rt, qt - rt' - i(rt)') = 1$ for all $i \in \mathbb{N}$. In the case $\deg(t) = 0$ the claim is obvious. Suppose $\deg(t) > 0$. Suppose otherwise and let $i \in \mathbb{N}$ be such that $g := \gcd(rt, qt - rt' - i(rt)') \neq 1$ and $s \in C[x]$ be an irreducible factor of g. Then $s \mid rt$ implies that either $s \mid r$ or $s \mid t$. We show that both are impossible. First, if $s \mid t$, then $s \mid qt - rt' - i(rt)' = qt - rt' - ir't - irt'$ implies $s \mid -(i+1)rt'$, which together with $s \nmid r$ and $i \in \mathbb{N}$ yields $s \mid t'$. Since t is squarefree, this contradicts $s \mid t$. Secondly, if $s \mid r$ then $s \mid qt - rt' - ir't - irt'$ implies $s \mid qt - ir't$, which together with $s \nmid t$ implies $s \mid q - ir'$, but then $s \mid \gcd(r, q - ir') = 1$, which is also impossible.

19. a. True. This follows directly from the definition. **b.** False. Counterexample: the rational function $h = 1/x$ is not a kernel, but its Gosper form is $(p, q, r) = (1, x, x)$.

20. a. $\frac{2(2n+1)}{n+1} - 1$; **b.** $3(3n+1)(3n+2)\binom{3n}{2n}$; **c.** $\frac{n+x+1}{n-x+1}\binom{n}{n-x}\binom{n+x}{x}$; **d.** $\frac{2(n+1)}{2n+1}(-4)^n\binom{2k}{k}^{-1} + 1$.

21. To be specific, consider the differential case. The shift case is analogous. Let f be the integrand and $u \in C(x)$ be such that $f'/f = u$. Let p, q, r be such that $u = q/r + p'/p$ is a Gosper form of u. The Gosper equation has several solutions if and only if there is a $y_h \in C[x]$ such that $ry'_h + (q + r')y_h = 0$. We can rewrite this to $q = -(r'y_h + ry'_h)/y_h$. Then $u = q/r + p'/p = -(r'y_h + ry'_h)/(ry_h) + p'/p = -r'/r - y'_h/y_h + p'/p$, which implies that $f = cp/(y_h r)$ for some constant c. In other words, the non-uniqueness of the solution of the Gosper equation implies that the integrand is rational.

In this case, if y_1 is some specific solution of the Gosper equation, the general solution is $y = y_1 + \alpha y_h$ for any constant α. The algorithm outputs

$$wf = \frac{r(y_1 + \alpha y_h)}{p}\frac{p}{y_h r} = \frac{y_1}{y_h} + \alpha,$$

so the non-uniqueness translates into the arbitrary choice of an additive constant in the indefinite integral.

Note that if the integrand is hyperexponential but not rational, we do not have the freedom to add a constant because then g and α are not similar, so $g+\alpha$ is only hyperexponential for $\alpha=0$.

22. With $f(k)=p(k)/k!$ we have $\frac{f(k+1)}{f(k)}=\frac{p(k+1)}{p(k)}\frac{1}{k+1}$, which leads to the Gosper equation $y(x+1)-xy(x)=p(x)$ where both y and p are undetermined. If we make an ansatz $p=p_0+p_1x+\cdots+p_dx^d$ with undetermined coefficients $p_0,\dots,p_d$, we can use Algorithm 3.56 to find all solutions $(y,p_0,\dots,p_d)\in C[x]\times C^{d+1}$ of the equation $y(x+1)-xy(x)=p_0+\cdots+p_dx^d$. With $d=0$ there is no nonzero solution, and for $d=1$ we find the solution $(y,p_0,p_1)=(-1,-1,1)$, so $p=x-1$ is an answer.

23. **a.** $-\frac{q^{n+1}}{1-q^{n+2}}(-1)^n\binom{2n+2}{n+1}_q+\frac{q}{1-q}$; **b.** $q^{(n+1)^2}(1-q^{n+1})\binom{2(n+1)}{n+1}_q+q^3-q$; **c.** $q^{(n+2)(n+1)/2}-1$; **d.** $\frac{1+q^{n+1}}{1-q^{n+1}}\binom{2(n+1)}{n+1}_q^{-1}-\frac{1}{1-q}$.

24. $x(0)+x(a-n)(-1)^n\prod_{i=1}^n\frac{x(a-i+1)}{x(i)}$. This identity appears in Apéry's proof of the irrationality of $\zeta(3)$ [439]. It is a variation of the more fundamental identity $\sum_{k=0}^n(x(k+1)-1)\prod_{i=1}^k x(i)=\prod_{k=1}^{n+1}x(k)-1$. A general summation theory for sums involving unspecified sequences is developed in [270, 271].

25. **a.** $\frac{2x^2+5x-4}{x^2(1-x)}K(x)-\frac{x+2}{x}K'(x)$; **b.** $\frac{-4x^2}{(1-x^2)^2}K(x^2)+\frac{2x^2}{1-x}K'(x^2)$; **c.** $-\frac{4(6175x^2+575x+79)}{27(x-1)x}K'(x)^2-\frac{4(24700x^3-3300x^2-676x-237)}{27(x-1)^2x^2}K'(x)K(x)-\frac{(154375x^4-32000x^3-656x^2-219x+1422)}{27(x-1)^3x^3}K(x)^2$.

26. **a.** $(n+1)H_n-n$; **b.** $2(3n+5)(2n+1)\binom{2n}{n}H_n-2(2n+1)\binom{2n}{n}+2$; **c.** $\frac14 n(n-3)+\frac12(1+n-n^2)H_n+\frac12 n(n+1)H_n^2$.

27. No, because $L^*\cdot v=1\iff L^*\cdot(-v)=-1$, so one equation is solvable if and only if the other is.

28. "$\Rightarrow$": If $\operatorname{rrem}(\Delta Q-p,L)=0$ then there is a $v\in K$ such that $\Delta Q-p=vL$. Then $Q^*\Delta^*-p=L^*v$, using $p=p^*$ and $v=v^*$. Applying these operators to 1 gives $-p=L^*\cdot v$.

"$\Leftarrow$": Let $v\in K$ be such that $L^*\cdot v=-p$, and let $Q=\operatorname{rquo}(vL,\Delta)$, so that $vL=\Delta Q+u$ for some $u\in K$. Taking adjoints gives $L^*v=Q^*\Delta^*+u$, and applying both sides of the equation to 1 gives $-p=L^{\cdot}v=0+u$, so we have $u=-p$, as desired.

29. The given recurrence translates into the annihilating operator $L=(x+4)\Delta^2+3\Delta-4(x+1)$, the adjoint of which can be written as $L^*=(5-3x)-(2x+3)S^{-1}+(x+2)S^{-2}$. According to the previous exercise, the summation problem has a solution if and only if there is a $v\in C(x)$ such that $L^*\cdot v=p$. Make an ansatz $p=c_0+c_1x+c_2x^2$ with undetermined coefficients and solve the resulting parameterized recurrence. This gives the solution $(v,p)=(1,-4x-12)$, so $p=x-3$ is a possible answer.

30. The integrand $\log(1-t)/t$ has the annihilating operator $L = t(t-1)D^2 + (3t-2)D + 1$, and since $\log(1-t)/t$ is obviously not hyperexponential, this must be an annihilating operator of minimal order. Since the equation $L^* \cdot v = -1$ has no solution v in $C(x)$, the claim follows directly from Proposition 5.10.

31. $m \in C(x)$ is such that $L^* \cdot m = -1$ if and only if there is a $Q \in C(x)[S]$ such that $mL = (S-1)Q-1$. As Gosper's algorithm returns $g = wf$ with $w = ry/p$, we can take $Q = ry/p$. Then $(S-1)ry/p - 1 = \frac{\sigma(r)\sigma(y)}{\sigma(p)}S - \frac{ry+p}{p} = \frac{\sigma(r)(ry+p)}{q}S - \frac{ry+p}{p}$, where we used $q\sigma(y) - ry = p$ in the second step. Comparison with the coefficients of $mL = m\sigma(r)pS - m\sigma(p)q$ yields $m = \frac{p+ry}{p\sigma(p)q}$, regardless of whether we look at the coefficient of S^0 or the coefficient of S^1.

32. "$\Rightarrow$": If v is such that $L^* \cdot v = 0$, then it follows directly from Lagrange's identity that $vL = \Delta Q$ for some $Q \in K[\Delta]$.

"$\Leftarrow$": By division with remainder, we can write $vL = \Delta Q + q$ for some $Q \in K[\Delta]$ and some $q \in K$. We show that $q = 0$. Indeed, $vL = \Delta Q + q$ implies $L^*v = Q^*\Delta^* + q$ (using $v^* = v$ and $q^* = q$), and applying the operators on both sides to 1 gives $L^* \cdot v = (L^*v) \cdot 1 = q \cdot 1 = q$. By assumption $L^* \cdot v = 0$, so $q = 0$, as claimed.

Section 5.2

1. **a.** $(D_x^{-1}D_x \cdot f)(x) = (D_x^{-1} \cdot f')(x) = \int_0^x f'(t)dt = f(x) - f(0)$. This is only equal to f if $f(0) = 0$. **b.** If g is an antiderivative of f, then $(D_x D_x^{-1} \cdot f)(x) = D_x \cdot \int_0^x f(t)dt = D_x \cdot (g(x) - g(0)) = f(x)$, so $D_x D_x^{-1} = \mathrm{id}$ seems to be a fair assumption. **c.** Since the answers to the previous two parts differ, it is better not to assume that D_x commutes with D_x^{-1}.

2. It is clear that $g = -\frac{1}{x-301} \in C(x)$ is a solution of the telescoping equation $\sigma(g) - g = \frac{1}{(x-300)(x-301)}$. By summing the equation $-\frac{1}{k-300} + \frac{1}{k-301} = \frac{1}{(k-300)(k-301)}$ for $k = 0, \ldots, n$ we indeed get $-\frac{1}{301} - \frac{1}{n-300} = \sum_{k=0}^n \frac{1}{(k-300)(k-301)}$, provided that such a summation is meaningful. While there is no trouble for $n < 300$, we cannot sum the equation for any larger choice of n, so even though the proposed closed form $-\frac{1}{301} - \frac{1}{n-300}$ can be evaluated for $n > 300$, the sum is not meaningful for these values.

3. "$\Rightarrow$" is clear, because the arguments of the gamma factors in Definition 5.13 are integer-linear and the denominator can only originate from those. For "$\Leftarrow$", note that $\frac{1}{an+bk+c} = \frac{\Gamma(an+bk+c)}{\Gamma(an+bk+c+1)}$ and observe that the product of any two proper hypergeometric terms is proper hypergeometric.

4. No. For example, $\frac{1}{n^2+k^2}$ is not holonomic, and $f(n,k) = \Delta_k \frac{1}{n^2+k^2} = \frac{1}{n^2+(k+1)^2} - \frac{1}{n^2+k^2}$ is not holonomic either (because if it were, closure properties would imply that $\frac{1}{n^2+k^2}$ is holonomic as well). Now $P = 1$ is a telescoper for $f(n,k)$ because $f(n,k) = \Delta_k \frac{1}{n^2+k^2}$ implies $(1 - \Delta_k \frac{1}{f(n,k)(n^2+k^2)}) \cdot f(n,k) = 0$.

5. If P and Q are such that $P - \partial_x Q \in I$, then $P - \partial_x(Q + L) \in I$ for every $L \in I$.

6. **a.** False. In fact, $\Gamma(n/2+k/3)$ is not even hypergeometric. To see this, note that $\Gamma((n+1)/2 + k/3)/\Gamma(n/2+k/3)$ behaves like $\sqrt{n/2}$ for fixed k and $n \to \infty$, and there is no rational function $r(n,k)$ with this growth rate. **b.** True: $n^{\underline{k}}$ can be identified with $\frac{\Gamma(n+1)}{\Gamma(n+1-k)}$. **c.** False: $h = n^2 + k^2$ is proper hypergeometric but $1/h$ is not. It is true however that the reciprocal of a proper hypergeometric term with $p = 1$ is a proper hypergeometric term. **d.** True: If h is such a term, then $\sigma(h)/h$ is a univariate rational function, and since C is algebraically closed, this rational function can be written as $\phi(n-a_1)^{e_1}\cdots(n-a_M)^{e_M}$ for some $\phi, a_1, \ldots, a_M \in C$ and $e_1, \ldots, e_M \in \mathbb{N}$. Then h can be written as $c\phi^n \Gamma(n-a_1)^{e_1}\cdots\Gamma(n-a_M)^{e_M}$ for some $c \in C$.

7. By multiplying the expression stated for $(S_n^i S_k^j \cdot h)/h$ in the proof by the denominator d we see that each term $S_n^i S_k^j$ in the ansatz for L contributes a polynomial of degree

$$i \underbrace{\sum_{m=1}^{M}(a_m + b_m - u_m - v_m)}_{=:\alpha}$$
$$+ j \underbrace{\sum_{m=1}^{M}(a'_m + v'_m - u'_m - b'_m)}_{:=\beta} + r \underbrace{\sum_{m=1}^{M}(u_m + u'_m + v_m + b'_m)}_{=:\gamma}.$$

The sum of all these polynomials for $i, j = 0, \ldots, r$ is a polynomial whose degree is at most $\max_{i,j=0}^{r}(\alpha i + \beta j + \gamma r) \le r(\gamma + \max(0,\alpha) + \max(0,\beta))$, as claimed.

8. The common denominator is $d = \prod_{m=1}^{M} U_m^{\overline{ru_m + su'_m}} V_m^{\overline{rv_m}} (B_m - sb'_m)^{\overline{sb'_m}}$ and the degree of the numerator of $(L \cdot h)/h$ is bounded by

$$\underbrace{\deg_k(p)}_{=:\delta} + \underbrace{r\sum_{m=1}^{M}(a_m + b_m + u_m + v_m)}_{=:\alpha} + \underbrace{s\sum_{m=1}^{M}(a'_m + b'_m + u'_m + v'_m)}_{=:\beta}.$$

The number of unknowns is $(r+1)(s+1)$, so the linear system obtained from comparing coefficients will have a solution as soon as $\delta + \alpha r + \beta s < (r+1)(s+1)$. The choice $r = \beta$, $s = \delta + (\alpha - 1)\beta$ meets this requirement.

9. **a.** We have $f(x) = \frac{\pi x \coth(\pi x) - 1}{2x^2}$, and this cannot be D-finite because it has infinitely many singularities (in $\mathbb{C}$). **b.** We have $a_n = \log(n+1) - \log(n)$, and if this were D-finite, then also $\log(n)$ would be D-finite, which by Exercise 8 of Sect. 2.4 is not the case.

10. **a.** $(-1)^n \binom{2n}{n}\binom{3n}{n}$; **b.** $(-1)^n \binom{2n}{n}$; **c.** $2n + 1$; **d.** 0; **e.** $2^{-n}\binom{2n}{n}$; **f.** $12(16^{-n}) \frac{(3n-1)!}{(n-1)!(3/2)^{\overline{n-1}}}$; **g.** $(-1)^{n+1}$; **h.** $(-x)^{\underline{n}}$; **i.** $(-1)^n/(2n + 1)$; **j.** $4^n/\binom{2n}{n}$; **k.** 2^{n+1}; **l.** $\binom{2n}{n}/4^n$. These and many other identities of a similar kind can be found in [222].

11. **a.** $\pi t/2$; **b.** $\frac{2\Gamma(1/3)\Gamma(7/6)}{\sqrt{\pi}} t^{-1/6}$; **c.** $2/(1 + 2n)$; **d.** $\exp(t^3/3)$; **e.** $\frac{1}{a}\sqrt{\frac{b}{a+b}}$; **f.** $1/t$.

12. For example, $F(n) = \sum_k \binom{n}{k}^3$ is annihilated by $P = (2 + n)^2 S_n^2 - (16 + 21n + 7n^2)S_n - 8(1 + n)^2$, and as it can be shown by the methods of Sect. 2.6 that P has no hypergeometric solutions, it follows that $F(n)$ is not hypergeometric.

13. For all three integrals, the substitution $x = \arcsin(y)$ leads to a D-finite integrand. **a.** Here the integral becomes $W_n = \int_0^1 \frac{y^n}{\sqrt{1-y^2}} dy$. Its integrand is annihilated by $(n+2)S_n^2 - (n+1) - D_y(y(1-y^2))$. Consequently, $((n+2)S_n^2 - (n+1)) \cdot W_n = 0$. **b.** Here the integral becomes $K(t) = \int_0^1 \frac{(1-t^2y^2)(1-y^2)}{d} y$. Its integrand is annihilated by an operator which translates into a telescoper of order 4. **c.** Here, we first shift the integration variable by $\pi/2$ to adjust the boundaries of the integral. Then the integral becomes

$$\begin{aligned} J_n(t) &= \int_{-\pi/2}^{\pi/2} \cos(n(x + \pi/2) - t\cos(x))dx \\ &= \int_{-1}^{1} \frac{\cos(n(\arcsin(y) + \pi/2) - t\sqrt{1 - y^2})}{\sqrt{1 - y^2}} dy. \end{aligned}$$

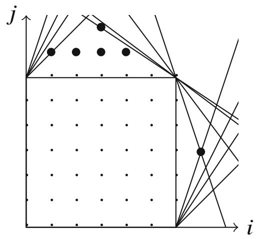
The integrand is recognized as being D-finite using closure properties and trigonometric addition theorems $\cos(u+v) = \cos(u)\cos(v) - \sin(u)\sin(v)$ and $\sin(u+v) = \sin(u)\cos(v) + \cos(u)\sin(v)$. In the resulting ideal, we can find operators whose coefficients are free of y. They give rise to nonzero telescopers, and the resulting telescopers generate an ideal for which it can be checked by a Gröbner basis computation that it is D-finite.

14. For the left hand side, we find an annihilating operator of order 4 and degree 5. The right hand side is annihilated by the operator $(2+n)^3 S_n^2 - (3+2n)(39+51n+17n^2)S_n + (1+n)^3$. The operator for the left hand side turns out to be a left multiple of this operator, so the larger operator annihilates both sides. For $n = 0, \ldots, 3$, both sides evaluate to 1, 5, 73, 1445, respectively. It follows that they agree for all n. This identity is taken from [419].

15. Suppose f is annihilated by an operator of the form $P - xQ$ with $P \in C[t][D_t]$ and $Q \in C[x,t][D_x, D_t]$. Setting $x = 0$ in the relation $(P - xQ) \cdot$

$f(x,t) = 0$ gives $P \cdot f(0,t) = (xQ \cdot f)|_{x=0} = 0$, so P is an annihilating operator of $f(0,t)$. To show that f has an annihilating operator of the form $P - xQ$ with $P \neq 0$, observe first that holonomy implies the existence of a nonzero annihilating operator L in $C[t,x][D_t]$ and then use Lemma 5.19 to show that there is a $k \in \mathbb{N}$ such that an $D_x^k L$ can be written as $P - xQ$ for some $P \neq 0$.

16. Every factor $\Gamma(an \pm bn)^{\pm 1}$ is annihilated by $1 - S_n^b S_k^{\mp a}$, so for every point (i,j) in the support of L, adding any term $S_n^u S_k^v$ with (u,v) on the line $(i,j) + \mathbb{Z}(b, \pm a)$ does not change the contribution of this term to the rational function. Moreover, all terms $S_n^u S_k^v$ with (u,v) on one side of this line correspond to a smaller contribution and may therefore be added as well—which side it is depends on the sign of b and of the exponent. More precisely, using the notation of the proof of Theorem 5.14 and an ansatz $L = \sum_{i=0}^r \sum_{j=0}^r \ell_{i,j} S_n^i S_k^j$, we can safely add all terms $S_n^i S_k^j$ with (i,j) such that $i \geq 0$, $j \geq 0$, $a_m(i-r) + a'_m(j-r) \leq 0$, $u_m(i-r) + u'_m(j-r) \leq 0$, $b_m(i-r) + b'_m j \leq 0$, $v_m(i-r) + v'_m j \leq 0$, $b_m i + b'_m(j-r) \geq 0$, and $v_m i + v'_m(j-r) \geq 0$, for all $m = 1, \ldots, M$. In the example under consideration, these are the terms $S_n S_k^7$, $S_n^2 S_k^7$, $S_n^2 S_k^8$, $S_n^3 S_k^7$, $S_n^3 S_k^8$, $S_n^4 S_k^7$, $S_n^7 S_k^3$.



17. If P and P' are in T and $Q_1, \ldots, Q_n, Q'_1, \ldots, Q'_n$ are such that $P - \sum_{i=1}^n \partial_{x_i} Q_i \in I$ and $P' - \sum_{i=1}^n \partial_{x_i} Q'_i \in I$ then $(P + P') - \sum_{i=1}^n \partial_{x_i}(Q_i + Q'_i) \in I$, so $P + P' \in T$. Moreover, for every $L \in C(t_1, \ldots, t_m)[\partial_{t_1}, \ldots, \partial_{t_m}]$ we have $LP - \sum_{i=1}^n \partial_{x_i} L Q_i \in I$, because L commutes with each ∂_{x_i}. Therefore $LP \in T$.

18. **a.** True. Let $P := P_1 \oplus P_2 = \operatorname{lclm}(P_1, P_2)$. By Exercise 17, there are $Q_1, Q_2 \in C(x,t)[\partial_x, \partial_t]$ such that $(P - \partial_x Q_1) \cdot f_1 = (P - \partial_x Q_2) \cdot f_2 = 0$. Let $U_1, U_2 \in C(x,t)[\partial_x]$ or $U_1, U_2 \in C(x,t)[\partial_t]$ be such that $1 = U_1 L_1 + U_2 L_2$. The existence of such operators follows from the assumption $\operatorname{gcrd}(L_1, L_2) = 1$. Now we can use a similar construction as in the proof of the Chinese remainder theorem. Set $Q = Q_1 + (Q_2 - Q_1) U_1 L_1$, so that $Q \cdot f_1 = Q_1 \cdot f_1$ and $Q \cdot f_2 = (Q_1 + (Q_2 - Q_1) U_1 L_1) \cdot f_2 = (Q_1 + (Q_2 - Q_1)(1 - U_2 L_2)) \cdot f_2 = Q_2 \cdot f_2$. Then $(P - \partial Q)(f_1 + f_2) = ((P - \partial Q) \cdot f_1) + ((P - \partial Q) \cdot f_2) = ((P - \partial Q_1) \cdot f_1) + ((P - \partial Q_2) \cdot f_2) = 0$. This shows that P is a telescoper for $f_1 + f_2$. **b.** False. For example, $S_n - 2$ is a telescoper for $\binom{n}{k}$ but $S_n - 4 = (S_n - 2)^{\otimes 2}$ is not a telescoper for $\binom{n}{k}^2$. This can be checked by applying Gosper's algorithm to $(S_n - 4) \cdot \binom{n}{k}^2 = -\frac{(-2k+n+1)(-2k+3n+3)}{(-k+n+1)^2} \binom{n}{k}^2$.

19. Let Q be a certificate of P, so that $(P - \partial_x Q) \cdot f = 0$. Then $(P - \partial_x Q) \cdot h^{-1} h f = 0$. Since h is hypergeometric/hyperexponential, so is h^{-1}. If $r_j \in C(t)$ is such that $\partial_t^j \cdot h^{-1} = r_j h^{-1}$ ($j \in \mathbb{N}$), then for every g we have $\partial_t^j \cdot h^{-1} g = h^{-1}(r_j \partial_t^j \cdot g)$. Moreover, since h does not depend on x, we have $\partial_x^i \cdot h^{-1} g = h^{-1}(\partial_x^i \cdot g)$ for every $i \in \mathbb{N}$ and every g. Therefore, if $\tilde{P}$, $\tilde{Q}$ are obtained from P, Q by replacing each term $\partial_x^i \partial_t^j$ with $r_j \partial_x^i \partial_t^j$, then for every g we have $(P - \partial_x Q) \cdot h^{-1} g = h^{-1}((\tilde{P} - \partial_x \tilde{Q}) \cdot g)$. In particular, $(\tilde{P} - \partial_x \tilde{Q}) \cdot hf = 0$. Note that $\tilde{P} \neq 0$ because all of the r_j are different from 0. Note that we also have $\tilde{P} = P \otimes (\partial_t - (\partial_t \cdot h)/h)$.

20. It follows from Theorem 5.14 that there are nonzero annihilating operators $L \in C[n][S_n, S_k]$. Among them, choose one whose degree with respect to S_k is minimal and let $P \in C[n][S_n]$, $Q \in C[n][S_n, S_k]$ be such that $L = P - (S_k - 1)Q$. We show that $P \neq 0$. Suppose otherwise. Then $(S_k - 1)Q$ is an annihilating operator of the term f under consideration. By the minimality assumption, Q cannot be an annihilating operator, so $h := Q \cdot f$ is a nonzero hypergeometric term which is constant with respect to S_k. Since $Q \cdot f$ is similar to f, there is a rational function u such that $Q \cdot f = uf = h$, so $f = u^{-1}h$, which is exactly the form that f is not supposed to have.

Section 5.3

1. If f and g are univariate D-finite functions, we can also view them as bivariate D-finite functions which are constant with respect to a second variable. Using closure properties, it then follows that the bivariate function $(x, t) \mapsto f(x)g(t - x)$ is D-finite. In the differential case, D-finiteness is preserved by definite integration. The claim follows. Note that we have already shown the discrete counterpart of this result in Sect. 2.3.

2. For $b_n = \sum_k \binom{n}{k} a_k$ we have $\sum_k (-1)^{n+k} \binom{n}{k} b_k = a_n$, because

$$\sum_k (-1)^{n+k} \binom{n}{k} \sum_i \binom{k}{i} a_i = \sum_i \left(\sum_k (-1)^{n+k} \binom{n}{k} \binom{k}{i} \right) a_i$$

and $\sum_k (-1)^{n+k} \binom{n}{k} \binom{k}{i} = \delta_{n,i}$ for all $n, i \in \mathbb{N}$. Since $(b_n)_{n=0}^{\infty}$ is D-finite by assumption, $(-1)^{n+k} \binom{n}{k} b_k$ is holonomic, so $\sum_k (-1)^{n+k} \binom{n}{k} b_k = a_n$ is holonomic, as claimed.

3. False. For example, for $f = 1$ and $g = \exp(x) - 1$ we have $a_{n,k} = \frac{n!}{k!} S_2(k, n)$, where $S_2(k, n)$ denotes the Stirling number of the second kind. If $a_{n,k}$ were D-finite, the Stirling numbers would be D-finite as well. This is not the case.

4. In the notation of Lemma 5.19, we have $R = C[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, D_{x_1}, \ldots, D_{x_n}]$ and $A = R[x_i]$. In the differential case, the functions σ, δ are defined so that $x_i D_{x_i} = D_{x_i} x_i - 1$ and x_i commutes with all x_j and D_{x_j} for $j \neq i$. Thus $\delta(D_{x_i}) = -1$ and $\delta(\sigma^a(D_{x_i}) + \cdots + \sigma^b(D_{x_i})) = -(b - a)$ is a constant, as required. In the shift case, we have the commutation rule $x_i \Delta_{x_i} = (\Delta_{x_i} - 1)x_i - 1$, so the argument is the same.

5. By Exercise 5 of Sect. 4.5, holonomy of $(a_{n,k})_{n,k=0}^{\infty}$ w.r.t. $C[n,k][S_n, S_k]$ implies holonomy of the series $\sum_{n,k=0}^{\infty} a_{n,k} u^n v^k \in C[[u,v]]$ w.r.t. $C[u,v][D_u, D_v]$. For power series, holonomy is equivalent to D-finiteness (Theorem 4.69). Setting $v = xv$ gives $\sum_{n,k=0}^{\infty} a_{n,k} x^k u^n v^k \in C[[x,u,v]]$, which by Theorem 5.30 is D-finite w.r.t. $C[x,u,v][D_x, D_u, D_v]$. Again by Exercise 5 of Sect. 4.5, holonomy w.r.t. $C[x,u,v][D_x, D_u, D_v]$ is equivalent to holonomy w.r.t. $C[x,u,v][D_x, \theta_u, \theta_v]$, where $\theta_u = uD_u$ and $\theta_v = vD_v$. Since $L(x,u,v,D_x,\theta_u,\theta_v)$ is an annihilating operator of $\sum_{n,k=0}^{\infty} a_{n,k} x^k u^n v^k$ if and only if $L(x, S_n^{-1}, S_k^{-1}, D_x, n, k)$ is an annihilating operator of $a_{n,k}x^k$, the holonomy of $\sum_{n,k=0}^{\infty} a_{n,k} x^k u^n v^k$ w.r.t. $C[x,u,v][D_x,\theta_u,\theta_v]$ implies the holonomy of $a_{n,k}x^k$ w.r.t. $C[n,k,x][S_n,S_k,D_x]$.

6. We show that $x + y \in C((x,y))$ has no multiplicative inverse. Suppose for the contrary that $\sum_{i,j} a_{i,j} x^i y^j$ is a multiplicative inverse. Then $1 = (x+y)\sum_{i,j} a_{i,j} x^i y^j = \sum_{i,j} a_{i,j} x^{i+1} y^j + \sum_{i,j} a_{i,j} x^i y^{j+1} = \sum_{i,j} (a_{i-1,j} + a_{i,j-1}) x^i y^j$ implies the recurrence $a_{i-1,j} + a_{i,j-1} = 0$ for all i, j. Because of $a_{-1,0} + a_{0,-1} = 1$, either $a_{-1,0} \neq 0$ or $a_{0,-1} \neq 0$, or both are nonzero. If $a_{-1,0}$ is nonzero, the recurrence implies that the coefficients of $x^{-k-1}y^k$ are nonzero for all $k \in \mathbb{N}$, and if $a_{0,-1}$ is nonzero, the recurrence implies that the coefficients of $x^k y^{-k-1}$ are nonzero for all $k \in \mathbb{N}$. In either case, the element $\sum_{i,j} a_{i,j} x^i y^j$ cannot belong to $C((x,y))$, because this ring only contains series for which there is some $e \in \mathbb{Z}$ such that the series only contains terms $x^i y^j$ where both i and j are greater than e.

7. It depends on whether $\frac{1}{x^3(x^2-x-1)}$ is viewed as an element of $C((x))$ or of $C((x^{-1}))$. In the first case, the result is $\frac{1}{x^3(x^2-x-1)} - (-x^{-3} + x^{-2} - 2x^{-1} + 3)$, in the second case it is 0.

8. In order to keep the expressions small, we show the claims only for $n = 2$, $m = 0$, $\ell = 0$. The same calculations work in the general case. **a.** Writing $a(x_1,x_2) = \sum_{i_1,i_2} a_{i_1,i_2} x_1^{i_1} x_2^{i_2}$, we have

$$\operatorname{diag}_{x_1,x_2} a(x_1,x_2) = \operatorname{diag}_{x_1,x_2} \sum_{i_1,i_2} a_{i_1,i_2} x_1^{i_1} x_2^{i_2} = \sum_{k\in\mathbb{Z}} a_{k,k} x_2^k$$

by definition. Now $\frac{1}{x_1} a(x_1, \frac{x_2}{x_1}) = \sum_{i_1,i_2} a_{i_1,i_2} x_1^{i_1-i_2-1} x_2^{i_2}$, and extracting the coefficient of x_1^{-1} gives $\sum_{k\in\mathbb{Z}} a_{k,k} x_2^k$, as required. **b.** Writing $a(x_1,x_2) = \sum_{i_1,i_2} a_{i_1,i_2} x_1^{i_1} x_2^{i_2}$ and $b(x_1,x_2) = \sum_{j_1,j_2} b_{j_1,j_2} x_1^{j_1} x_2^{j_2}$ we have $a \odot_{x_1,x_2} b = \sum_{i_1,i_2} a_{i_1,i_2} b_{i_1,i_2} x_1^{i_1} x_2^{i_2}$ by definition. Now

$$a(x_1,x_2)b(\bar{x}_1,\bar{x}_2) = \sum_{i_1,i_2} \sum_{j_1,j_2} a_{i_1,i_2} b_{j_1,j_2} x_1^{i_1} x_2^{i_2} \bar{x}_1^{j_1} \bar{x}_2^{j_2},$$

so

$$\operatorname{diag}_{\bar{x}_1,x_1} \operatorname{diag}_{\bar{x}_2,x_2} a(x_1, x_2)b(\bar{x}_1, \bar{x}_2) = \sum_{i_1,i_2} a_{i_1,i_2} b_{i_1,i_2} x_1^{i_1} x_2^{i_2},$$

as required.

9. Because of $\operatorname{diag}_{x,y} f = \operatorname{Res}_x f(x, y/x)/x$, it suffices to show that this residue is algebraic. By Hermite reduction and Theorem 5.4, a rational function is integrable (in the sense that its integral is again a rational function) if and only if the residues at all its poles are zero. Therefore, if $L \in C(y)[D_y]$ is an annihilating operator for the residues of $f(x, y/x)/x$, viewed temporarily as elements of $C(y)(x)$, then $L \cdot f(x, y/x)/x = D_x \cdot g$ for some rational function g, and thus, now viewing f and g as series again, $L \cdot \operatorname{Res}_x f(x, y/x)/x = 0$. The residues of $f(x, y/x)/x$ at the poles of this rational function are algebraic, and if L is chosen to be of minimal order, then it only has algebraic solutions (Exercise 16 in Sect. 4.4). Therefore $\operatorname{Res}_x f(x, y/x)/x$ is algebraic.

This result is due to Furstenberg [199], who gives a shorter proof for the case $C = \mathbb{C}$ using a bivariate contour integral, and then discusses the case when C has positive characteristic. The algebraic proof given here appears in [131, Theorem 4.18].

10. As the operator Res_x is defined for series, not for rational functions, we must map $C(x, y)$ into a Laurent series field $C_{\leq}((x, y))$ in order to give a meaning to $\operatorname{Res}_x f$. This can be done in several ways, and in some of them, the residue of $\frac{b}{1+xc}$ may be nonzero. For example, $1/(1 - \frac{x}{y})$ admits the expansion $-\sum_{n=1}^{\infty}(y/x)^n$, and the residue of this series is y. This is nonzero, but still rational. An example with an irrational residue is $1/(1 - \frac{x}{y} - x^2)$ expanded like $-\frac{y}{x}\sum_{n=0}^{\infty}(\frac{(1-x^2)}{x})^n y^n$. Its residue with respect to x is the irrational series $y/\sqrt{1+4y^2} = \sum_{n=0}^{\infty}(-1)^{n+1}\binom{2n}{n}y^{2n+1}$.

11. a. We have $\operatorname{Res}_{y-\alpha} h = \alpha$ for each root α of m (Theorem 5.4), therefore $\operatorname{Res}_{y-a} h = a$, and therefore $\operatorname{Res}_y h(x, y+a) = a$. We show that $\operatorname{Res}_y h(x, y+a) = \operatorname{Res}_y h(x, y)$ for a suitable expansion of h. By assumption, m involves the terms x^1y^0 and x^0y^1. Choose a term order for which x^0y^1 is the smallest term. Then h has an expansion of the form $\sum_{n=0}^{\infty}(\frac{x}{y})^n p_n(x, y)$ for certain polynomials $p_n \in C[x, y]$. The exponent vectors (i, j) of the terms $x^i y^j$ in this series belong to the cone generated by $(0, 1)$ and $(1, -1)$. Writing the expansion of h as $\sum_{i,j} h_{i,j}x^i y^j$ implies that $h_{i,j} = 0$ if $i < 0$ or $i + j < 0$, and with this notation, we have $\operatorname{Res}_y h = \sum_i h_{i,-1}x^i$. In the series $h(x, y + a) = \sum_{i,j} h_{i,j}x^i(y + a)^j$, the chosen term order forces the expansions $(y + a)^j = \sum_{k=0}^{\infty}\binom{j}{k}a^k y^{j-k}$ (rather than $(y + a)^j = \sum_{k=0}^{\infty}\binom{j}{k}a^{j-k}y^k$, which would not contribute anything to the residue), so we get $h(x, y + a) = \sum_{k=0}^{\infty}\sum_{i,j} h_{i,j}\binom{j}{k}a^k x^i y^{j-k}$. This series is well-defined, because the only summands contributing to the coefficient of a term $x^u y^v$ are those with $j - k = v$, and $k + i \leq u$, and because of $i \geq 0$, $k \geq 0$, and $i + j \geq 0$, there are only finitely many of these summands. We now have $\operatorname{Res}_y \sum_{k=0}^{\infty}\binom{j}{k}a^k y^{j-k} =$

$\delta_{j,-1}$ for every j, so $\operatorname{Res}_y h(x, y+a) = \operatorname{Res}_y \sum_{i,j} \sum_{k=0}^{\infty} h_{i,j} x^i \binom{j}{k} a^k y^{j-k} = \sum_i h_{i,-1} x^i = \operatorname{Res}_y h(x, y)$, as claimed. **b.** Since $h = (yD_y \cdot m)/m = \frac{2y^2}{y^2 - x^2(x+1)}$ is even with respect to y, every expansion of h with only involve terms $x^i y^j$ with j even. Therefore, every expansion has a zero residue, and is thus different from the two series solutions of m.

12. For $r \in C(x)$, we have $[x^>]r(x, y) = r(x) - p(x^{-1})$ or $[x^>]r = p(x)$ for some polynomial p, depending on whether we interpret r with an element of $C((x))$ or $C((x^{-1}))$, and in either case, the result is rational. An example for the bivariate case was already given in Example 5.34.

13. **a.** As we have $a \odot_{x_n} (r_1 + r_2) = (a \odot_{x_n} r_1) + (a \odot_{x_n} r_2)$, it suffices to consider a single term of the partial fraction decomposition of r. For a term cx_n^e of the polynomial part of the partial fraction decomposition, we have $a \odot_{x_n} cx_n^e = (ce! D_{x_n}^e \cdot a)|_{x_n=0} x_n^e$, which is algebraic because evaluation and differentiation preserves algebraicity. For a partial fraction $\frac{c}{(1-\alpha x_n)^e} = c \sum_{k=0}^{\infty} \alpha^{k+e} (k+e)^{\underline{e}} x_n^k$, we have $a \odot_{x_n} \frac{c}{(1-\alpha x_n)^e} = cD_{x_n}^e \cdot a$, which is also algebraic. **b.** From $\frac{1}{1-(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})t} = \sum_{n=0}^{\infty} (\frac{x}{y} + \frac{y}{z} + \frac{z}{x})^n t^n = \sum_{n=0}^{\infty} \sum_k \sum_\ell \binom{n}{k}\binom{k}{\ell} x^{n-k-\ell} y^{2k-n-\ell} z^{2\ell-k} t^n$ it can be deduced that the nonnegative part is $\sum_{n=0}^{\infty} \binom{3n}{2n}\binom{2n}{n} t^{3n}$. This series is annihilated by $(3t-1)(9t^2+3t+1)tD_t^2 + (108t^3-1)D_t + 54t^2$. As this operator is irreducible and has a logarithmic singularity at zero, it does not have any algebraic solutions.

The result of part b is not a contradiction to part a because $\frac{1}{1-(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})t}$ is not an element of $C[[x, y, z, t]]$.

14. Yes, because $f(x_1, \dots, x_n, y_1, \dots, y_m) \odot_{x_1,\dots,x_n} g(x_1, \dots, x_n, \bar{y}_1, \dots, \bar{y}_m)$ is D-finite by the theorem if $\bar{y}_1, \dots, \bar{y}_m$ are fresh variables. Afterwards setting $\bar{y}_i$ to y_i for $i = 1, \dots, m$ preserves D-finiteness by Theorem 5.30.

15. Let $p, q \in \mathbb{Z}[[x_1, \dots, x_n]]$ be such that for an expansion g of p/q in some Laurent series field $\mathbb{Q}_{\leq}((x_1, \dots, x_n))$ we have $\operatorname{diag}_{x_1,\dots,x_n} g = f$ (identifying x with x_n). It is clear that

$$\operatorname{diag}_{x_1,\dots,x_n} \alpha g(\beta x_1, \dots, \beta x_n) = \alpha f(\beta^n x),$$

so it suffices to show that there are $\alpha, \beta \neq 0$ such that the series coefficients of $\alpha g(\beta x_1, \dots, \beta x_n)$ are integers. Let $c\tau$ be the smallest monomial in q with respect to $\leq$, so that $q = c\tau(1-\tilde{q})$ for $\tilde{q} = (c\tau - q)/(c\tau)$. Then $q^{-1} = c^{-1}\tau^{-1} \sum_{k=0}^{\infty} (\tilde{q})^k$, and by choosing β such that $\tilde{q}(\beta x_1, \dots, \beta x_n)$ has coefficients in $c\mathbb{Z}$, we can ensure that $cq^{-1}(\beta x_1, \dots, \beta x_n)$ has coefficients in $\mathbb{Z}$. For such a β and for $\alpha = 1/c$, it then follows that $\alpha g(\beta x_1, \dots, \beta x_n)$ has integer coefficients.

16. **a.** False. For example, for $f = g = \frac{1}{(1-x)(1-y)} = \sum_{n,k=0}^{\infty} x^n y^k$ we have $\operatorname{diag}(f) = \operatorname{diag}(g) = \frac{1}{1-x}$, so $\operatorname{diag}(f)\operatorname{diag}(g) = \frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + \cdots$, while $fg = \frac{1}{(1-x)^2(1-y)^2} \sum_{n,k=0}^{\infty} (n+1)(k+1) x^n y^k$

implies $\operatorname{diag}(fg) = \frac{x+1}{(1-x)^2} = 1 + 4x + 9x^3 + \cdots$. **b.** False. For example, for $f = \frac{1}{(1-x_1)(1-x_2)(1-x_3)(1-x_4)} \in C[[x_1, x_2, x_3, x_4]]$ we have $\operatorname{diag}_{x_1,x_2,x_3,x_4} = \frac{1}{1-x_4} \neq \frac{1}{(1-x_2)(1-x_4)} = \operatorname{diag}_{x_1,x_2} \operatorname{diag}_{x_3,x_4} f$. **c.** True, because if $f = \operatorname{diag}_{x_1,\dots,x_n} F(x_1, \dots, x_n)$ and $g = \operatorname{diag}_{y_1,\dots,y_m} G(y_1, \dots, y_m)$ for certain rational series F, G (identifying x with x_n and y_m), then

$$f \odot_x g = \operatorname{diag}_{x_1,\dots,x_n,y_1,\dots,y_m} F(x_1, \dots, x_n)G(y_1, \dots, y_m).$$

17. If we can compute positive parts, we can also compute nonnegative parts and negative parts, and using these, we can compute residues via $\operatorname{Res}_{x_1,\dots,x_n} a = a - [x_1^{\geq} \cdots x_n^{\geq}]a - \frac{1}{x_1 \cdots x_n}[x_1^{<} \cdots x_n^{<}]x_1 \cdots x_n a$.

18. $[x^0y^0](1 - \frac{x}{y})^n(1 - \frac{y}{x})^m = [x^0y^0]\sum_k \binom{n}{k}(-\frac{x}{y})^k \sum_\ell \binom{m}{\ell}\binom{m}{\ell}(-\frac{y}{x})^\ell = \sum_k \binom{n}{k}\binom{m}{k} = \binom{n+m}{n}$, as claimed. A proof of the general case can be found in [220]; some extensions and generalizations are given in [405, 471].

19. Denote the two series in question by $f(x, y)$ and $g(x, y, t)$, respectively. **a.** f is not D-finite. If it were, then also $f(x, y) - xf(x, y) = \sum_{n=0}^\infty x^{n^2} y^n$ would be D-finite, then also $\sum_{n=0}^\infty x^{n^2}$ would be D-finite. This cannot be the case, for the same reason as in Exercise 3 from Sect. 3.1. **b.** g is not D-finite either. If it were, then also $g(x, y, t) \odot_{x,y,t} \sum_{n=0}^\infty \sum_{i,j:n=i+1} x^i y^j t^n = \sum_{n=0}^\infty \sum_{j:j^2 \leq 2n-1} x^{n-1} y^j t^n$ would be D-finite. Replacing x by 1 and t by x^2, then dividing by x, and finally applying $[y^{\geq}]$ reduces the problem to part a.

20. $e_4 = \frac{1}{4}(\frac{1}{6}p_1^4 - p_1^2 p_2 + \frac{4}{3}p_1 p_3 + \frac{1}{2}p_2^2 - p_4)$.

21. According to the definition of D-finiteness for series in infinitely many variables, it suffices to show that for every fixed $n \in \mathbb{N}$ the series $\prod_{j=1}^n \prod_{i=1}^{j-1}(1 + x_i x_j)$ and $\prod_{j=1}^n \prod_{i=1}^{j-1} \frac{1}{1-x_i x_j}$ are D-finite. As these are rational functions, this is clearly the case.

22. By the way D-finiteness is defined for series in infinitely many variables, the series $f = \sum_{n=0}^\infty a_n p_n$ is D-finite regardless of its coefficients a_n, because setting all but finitely many of the p_n to zero gives just a polynomial. For the same reason, the series $g = \sum_{n=0}^\infty t^n p_n$ is D-finite. Now note that $\langle f|g\rangle = \sum_{n=0}^\infty a_n t^n$.

23. The question is whether the bivariate sequence $(c_{n,j})_{n,j=1}^\infty$ is D-finite. It turns out that $c_{n,j} = (-1)^{n+j}\binom{n-1}{j-1}^2/\binom{2n-2}{n-j}$ for $1 \leq j \leq n$, which is indeed D-finite.

Section 5.4

1. The results remain the same.

2. The results remain the same.

3. We can use $\frac{k-n+b}{k-n-1}\binom{b}{n-k} = \binom{b}{n+1-k}$ to rewrite the creative telescoping relation in the form

$$(n-a-b)f(n,k) + (n+1)f(n+1,k) = \Delta_k k\binom{a}{k}\binom{b}{n+1-k},$$

which is valid for all integers.

4. False. Counterexample: For $h = k2^n$ we have $(S_n - 2)\cdot h = \Delta_k \cdot 0$.

5. If h is a hypergeometric term that leads to such a solution, then we have a nonzero rational function Q such that $\Delta_k Qh = 0$. This means that Qh is a constant. This can happen for instance if h itself is a rational function, because in this case we can take $Q = 1/h$.

6. False. A counterexample is $h = (-1)^k\binom{2n}{k}^3$, which admits a telescoper of order 1 while the minimal telescoper of kh has order 2. Such examples are rare though.

7. If we replace mn with a new parameter j, then we can easily find the telescopers $(j+1-n)S_j - (j+1)$ and $(n+1)S_n - (n-j)$. Let I be the ideal generated by these operators in $C(n,j)[S_n, S_j]$. For setting j back to mn, we need an element of I which is a $C(n,j)$-linear combination of powers of $S_j^m S_n$. As $S_j^m S_n$ itself is equivalent modulo I to $-\frac{(j+m)^{\underline{m}}}{(n+1)(j+m-1-n)^{\underline{m-1}}}$, it follows that $(n+1)(mn+m-1-n)^{\underline{m-1}}S_n + (mn+m)^{\underline{m}}$ is a telescoper for h.

8. Writing $h = \frac{n^{\underline{mk}}}{(mk)!}$, we see that the differencing rule $\Delta_n n^{\underline{\alpha}} = \alpha n^{\underline{\alpha-1}}$ implies $\Delta_n^m \cdot h = \frac{(mk)^{\underline{m}}}{(mk)!}n^{\underline{mk-m}} = \frac{1}{(m(k-1))!}n^{\underline{m(k-1)}} = \binom{n}{m(k-1)}$. Therefore, $(1-\Delta_n^m)\cdot h(n,k) = \Delta_k \cdot h(n,k-1)$, and as $Q = h(n,k-1)/h(n,k)$ is a rational function in n and k, it follows that $T = 1 - \Delta_n^m$ is a telescoper.

9. For $f(n,k) = \frac{(-1)^k}{k+1}\binom{2k}{k}\binom{n+k}{2k+1}$ and $g(n,k) = \frac{k(-1)^{k+1}}{n(n+1)}\binom{2k}{k}\binom{n+k}{2k}$ we have $f(n+1,k) - f(n,k) = g(n,k+1) - g(n,k)$. For $G(k) = \sum_{n=1}^k g(n,k)$ it follows $f(k+1,k) - f(1,k) = G(k+1) - g(k+1,k+1) - G(k)$, i.e., $G(k+1) - G(k) = f(k+1,k) + g(k+1,k+1) = \frac{(5k+4)(-1)^k}{(k+1)(k+2)}\binom{2k}{k}$. The companion identity is therefore $\sum_{n=1}^k \frac{k(-1)^{k+1}}{n(n+1)}\binom{2k}{k}\binom{n+k}{2k} = 1 + \sum_{i=1}^{k-1}\frac{(5i+4)(-1)^i}{(i+1)(i+2)}\binom{2i}{i}$. It holds for $k \geq 1$. The sum on the right cannot be simplified any further.

10. Start from $f(n+1,k) - f(n,k) = g(n,k+1) - g(n,k)$ and exchange n and k to obtain $g(k,n+1) - g(k,n) = f(k+1,n) - f(k,n)$. Now replace k by $-k-1$ and n by $-n-1$ to obtain $g(-k-1,-n) - g(-k-1,-n-1) = f(-k,-n-1) - f(-k-1,-n-1)$. Therefore, $\tilde f(n+1,k) - \tilde f(n,k) = g(-k-1,-n-1) - g(-k-1,-n) = f(-k-1,-n-1) - f(-k,-n-1) = \tilde g(n,k+1) - \tilde g(n,k)$.

11. This example is taken from [351]. Like in creative telescoping, consider the application of Gosper's algorithm to an ansatz of the form $(c_0 + c_1 x + \cdots + c_s x^s)h$

with undetermined coefficients. Let $p, q, r \in C[x]$ be such that $\frac{\sigma(h)}{h} = \frac{\sigma(p)}{p} cq\sigma(r)$ is a Gosper form of h. Then the Gosper equation for $(c_0 + c_1 x + \cdots + c_s x^s)h$ will be $q\sigma(y) - ry = (c_0 + c_1 x + \cdots + c_s x^s)p$. The right hand side has degree $s + \deg(p)$, and if we choose $y = y_0 + \cdots + y_d x^d$ with $d = s + \deg(p) - \max(\deg(q), \deg(r))$, the degree of the left hand side is not more than $s + \deg(p)$, so equating like terms leads to a linear system with at most $s + \deg(p) + 1$ equations and $(s + 1) + (s + \deg(p) - \max(\deg(q), \deg(r)) + 1)$ equations, and this system will have a nontrivial solution if we choose $s \geq \max(\deg(p), \deg(q))$.

12. It suffices to consider the polynomials $p = x^{\underline{m}}$, because they form a basis of $C[x]$. The summand $f(n,k) = k^{\underline{m}}\binom{n}{k}$ satisfies the creative telescoping relation $(n+1-m)f(n+1,k) - 2(n+1)f(n,k) = (k+1)^{\underline{m}}\binom{n+1}{k+1} - k^{\underline{m}}\binom{n+1}{k}$, which implies that the sum $F(n) = \sum_k k^{\underline{m}}\binom{n}{k}$ satisfies the recurrence $(n+1-m)F(n+1) - 2(n+1)F(n) = 0$. Up to a constant multiple, the sum must therefore be equal to $n^{\underline{m}} 2^n$.

13. One expansion is $\frac{1}{1-(\frac{x^2}{t}+\frac{t^2}{x})} = -\frac{t}{x^2}\frac{1}{-\frac{t}{x^2}+1+\frac{t^3}{x^3}} = -\frac{t}{x^2}\sum_{n=0}^{\infty}(\frac{t}{x^2} - \frac{t^3}{x^3})^n$, as it only involves powers of x with exponents less than -2, its residue is zero. By symmetry, another expansion is $-\frac{x}{t^2}\sum_{n=0}^{\infty}(\frac{x}{t^2} - \frac{x^3}{t^3})^n$, and as this series only involves powers of x with positive exponents, its residue is zero too. A nonzero residue appears for the expansion $\sum_{n=0}^{\infty}(\frac{x^2}{t} + \frac{t^2}{x})^n$.

14. For example, the term $h(n,k) = k\binom{n}{k}^3$ has a telescoper of order 3, while $h(n,k) + h(n,n-k) = n\binom{n}{k}^3$ has a telescoper of order 2. It has been proposed in [350] to use this observation for simplifying difficult summation problems in the q-case.

15. Using $P_n(-1) = (-1)^n$ and $P_n(1) = 1$ we get

$$\int_{-1}^{1} D_x \cdot \big(xP_n(x)^2 - 2P_n(x)P_{n+1}(x) + xP_{n+1}(x)^2\big)dx$$
$$= \big[xP_n(x)^2 - 2P_n(x)P_{n+1}(x) + xP_{n+1}(x)^2\big]_{x=-1}^{1}$$
$$= -1 - 2(-1) - 1 - (1 - 2 + 1) = 0,$$

as claimed.

16. Let $f(n,k) = \sum_{i=0}^{k}\binom{n}{i}$ and $F(n) = \sum_{k=0}^{n} f(n,k)^3$. From $f(n,k+1) - f(n,k) = \binom{n}{k+1}$ we get that $((k+2)S_k + (k+1-n))(S_k - 1) = (k+2)S_k^2 - (n+1)S_k + (n-k-1)$ annihilates $f(n,k)$. Another annihilating operator for $f(n,k)$ can be found with creative telescoping. From the creative telescoping relation for $\binom{n}{i}$ derived in Examples 5.41 and 5.42, we get $f(n+1,k) - 2f(n,k) = -\frac{k+1}{n+1}\binom{n+1}{k+1}$, so $((n+1-k)S_n - (n+1))(S_n - 2) = (n+1-k)S_n^2 - (3n+3-2k)S_n + 2(n+1)$ annihilates $f(n,k)$. Let I be the ideal generated by these two operators in $C(n,k)[S_n,S_k]$. Using closure properties, we can compute from I a D-finite ideal J of annihilating operators for $f(n,k)^3$. Chyzak's algorithm applied to $1 \in C(n,k)[S_n,S_k]/J$ finds the telescoper $P=(n+1)S_n^2-(7n+12)S_n-4(2n+1)$ and a somewhat lengthy certificate Q. If we choose the equivalence classes of $S_n^3S_k$, $S_n^2S_k$, S_n^3, S_n^2 as basis of $C(n,k)[S_n,S_k]/J$, the common denominator of the coefficients of the certificate is $(2n+5-k)(n+1)^3(n+2)^3(n+3)$, so there is no trouble with singularities for this choice. This basis was found by trial and error, after observing that other bases lead to troublesome denominators.

We still have to deal with the non-natural boundaries of the outer sum $F(n)$. Summing $(P-\Delta_k Q)\cdot f(n,k)=0$ for k from -1 to n gives $(n+1)(F(n+2)-f(n+2,n+2)^3-f(n+2,n+1)^3)-(7n+12)(F(n+1)-f(n+1,n+1)^3)-4(2n+1)F(n)=(Q\cdot f^3)|_{k=n+1}-(Q\cdot f^3)|_{k=-1}=-(n+1)f(n+2,n+1)^3+\frac{1}{32}(5n+6)f(n+2,n+2)^3$, which simplifies to $(P\cdot F)(n)=-(7n+12)f(n+1,n+1)^3+\frac{37n+38}{32}f(n+2,n+2)^3=(9n-10)2^{3n+1}$. Now we use the techniques from Sect. 2.6 to find the hypergeometric solutions of this recurrence, and match their initial values to those of $F(n)$. The final result is $F(n)=(n+2)2^{3n-1}-3n2^{n-2}\binom{2n}{n}$. This identity first appeared in [121].

17. For the first sum, Zeilberger's algorithm finds the telescoper $(n+2)^3S_n^2-(2n+3)(17n^2+51n+39)S_n+(n+1)^3$, and since the sum has natural boundaries, this is also an annihilating operator for the sum. The second sum requires more work. Viewing $\sum_{i=1}^n \frac{1}{i^3}$ as a bivariate sequence in n and k, we have the annihilating operators S_k-1 and $(n+2)^3S_n^2-(2n+3)(n^2+3n+3)S_n+(n+1)^3$, where the latter can be obtained from $\sum_{i=1}^{n+1}\frac{1}{i^3}-\sum_{i=1}^n\frac{1}{i^3}=\frac{1}{(n+1)^3}$. We thus have a D-finite annihilating ideal in $C(n,k)[S_n,S_k]$ for the first inner sum. For the second sum, we can get the annihilating operator $(k+2)(k-n+1)(k+n+2)S_k^2+(-2k^3-8k^2+kn^2+kn-11k+2n^2+2n-5)S_k+(k+1)^3$ in the same way. A second recurrence can be found with creative telescoping, as follows. The creative telescoping operator $(S_n-1)-(S_i-1)\frac{2i(n+1-i)}{(n+1)^2}$ implies an inhomogeneous recurrence for the sum $\sum_{i=1}^k \frac{(-1)^i}{2i^3\binom{n+1}{i}\binom{n+1+i}{i}}$ (which does *not* have natural boundaries). It follows that if L is an annihilator for the right hand side of this inhomogeneous recurrence, then $L(S_n-1)$ annihilates the sum. We have thus also found a D-finite annihilating ideal in $C(n,k)[S_n,S_k]$ for the second inner sum. Using closure properties, we can now compute a D-finite annihilating ideal for $\binom{n}{k}^2\binom{n+k}{k}^2\left(\sum_{i=1}^n\frac{1}{i^3}-\sum_{i=1}^k\frac{(-1)^i}{2i^3\binom{n}{i}\binom{n+i}{i}}\right)$ to which we can then apply Chyzak's algorithm. This yields a telescoper of order 4 with polynomial coefficients of degree 22. This telescoper is also an annihilating operator for the sum under consideration. Since this operator is a left multiple of the third order annihilating operator, we can conclude the proof by checking a few initial values. Alternatively, before calling Chyzak's algorithm, we can use guess-and-prove to find an additional annihilating operator for the summand. It turns out that there is one. Applying Chyzak's algorithm to the ideal with this relation added, we get the telescoper $(n+2)^3S_n^2-(2n+3)(17n^2+51n+39)S_n+(n+1)^3$.

The sums discussed here play a crucial role in Apéry's proof that $\zeta(3)$ is irrational. See [439] for details about this proof, and [390] for an alternative computer proof using summation algorithms based on difference field theory.

18. **a.** False. For example, if I is the annihilating ideal of the proper hypergeometric term $h = \binom{n}{k}^3$, then $\dim_{C(x,t)} C(x,t)[\partial_x, \partial_t]/I = 1$ but the minimal telescoper has order two, so $\dim_{C(t)} C(t)[\partial_t]/T = 2 > 1$. **b.** False. For example, if I is the annihilating ideal of the proper hypergeometric term $h = 2^k$, which is indefinitely summable, then $\dim_{C(x,t)} C(x,t)[\partial_x, \partial_t]/I = 1$ but the minimal telescoper is 1, so $\dim_{C(t)} C(t)[\partial_t]/T = 0 < 1$.

19. **a.** $(4n+3)(4n+5)I(n,t) + 8(n+1)(2n+3)(t^2-2)I(n+1,t) - 16(n+1)(n+2)(t-1)(t+1)I(n+2,t) = 0$; **b.** $4(t-1)(t+1)\frac{d^2}{dt^2}I(n,t) + 4(2n+3)t\frac{d}{dt}I(n,t) + (4n+3)I(n,t) = 0$. In both cases, the certificate part evaluates to zero.

20. If $a = 0$, then $\gcd(a,b) = 1$ forces $b = 1$, so we have $f = 1/(k+c)^m$ in this case, and $P \cdot f = (S_n - 1) \cdot f = 0$ shows that P is a telescoper. Now suppose that $a \neq 0$. To see that P is a telescoper in this case, observe that $\sigma_n^b(f) = \sigma_k^a(f)$, and that $\sigma_k^a(f) - 1$ can be written as $(S_k - 1) \cdot \sum_{i=0}^{a-1} \sigma_k^i(f)$ if $a > 0$, and as $(S_k - 1) \cdot \sum_{i=1}^{-a} (-1)^i \sigma_k^{-i}(f)$ if $a \le 0$. In each case, we have $P \cdot f = (S_k - 1) \cdot Q$ for some Q, so P is a telescoper.

It can further be shown that P is in fact the minimal telescoper if $\gcd(a,b) = 1$. This is Lemma 2 in [306], where a detailed analysis of the structure of telescopers for rational functions is given.

21. Suppose $P = c_0 + \cdots + c_s S_n^s$ is a telescoper. Then $P \cdot \frac{1}{nk+1}$ is a rational function whose denominator divides $\prod_{i=0}^{s}(nk+ik+1)$. Moreoever, since the terms $\frac{1}{nk+ik+1}$ are $C(n)$-linearly independent (as shown in Exercise 10 of Sect. 4.5), a factor $(nk+ik+1)$ appears in the denominator if and only if c_i is nonzero. Since P is supposed to be a telescoper, it is nonzero, so we have $c_i \neq 0$ for some i. Fix such an i. If $Q \in C(n,k)$ is such that $P \cdot \frac{1}{nk+1} = (S_k - 1) \cdot Q$, then the factor $(nk+ik+1)$ must appear in the denominator of $(S_k - 1) \cdot Q$. But then, there must be some $j \neq 0$ such that also $(nk+ik+jn+ij+1)$ appears in the denominator. This follows from the reasoning used in Sect. 2.5 in the context of constructing denominator bounds. As there is no such factor in the denominator of $P \cdot \frac{1}{nk+1}$, we obtain the desired contradiction.

22. In both cases we get the telescoper $(-1+t-t^2)D_t + (2t-1)$. The certificate is

$$\frac{(1-2t)(-4t^3+27t^4+42t^2x+27x^2-12tx^2-4x^3)}{6(t^2-3x+4tx)} D_t$$
$$+ \frac{t^2-16t^3+19t^4+8tx-11t^2x+8t^3x+7x^2-22tx^2+16t^2x^2}{3(t^2-3x+4tx)}$$

in the first case, and $\frac{1}{3}(2t-1)x + \frac{1}{3}(t^2+4tx-5t-2x)y + \frac{1}{2}(1-2t)y^2$ in the second case.

23. From Theorem 5.40 it only follows that the first application of Chyzak's algorithm finds a minimal telescoper for the inner sum/integral with respect to the integrand and that the second application of Chyzak's algorithm finds a minimal telescoper for the outer sum/integral with respect to the inner sum/integral. As shown in the text, any telescoper of the outer sum/integral with respect to the inner sum/integral is also a telescoper of the double sum/integral with respect to the summand/integrand, but the converse is not true. So the double sum/integral can have a telescoper which is not at the same time a telescoper of the outer sum with respect to the inner sum.

An example is $f = \frac{1}{(t-x_1)(t-x_2)}$. Integrating with respect to x_1, we get the telescopers $P_1 = (t - x_2)D_t + 1$ and $P_2 = (t - x_2)D_{x_2} - 1$. Applying Algorithm 5.44 to the element $1 \in C(t, x_1, x_2)[D_t, D_{x_1}, D_{x_2}]/\langle P_1, P_2\rangle$ gives the minimal telescoper D_t. This is however not a minimal telescoper for f because we also have $(1 - D_{x_1}(x_1 - t) - D_{x_2}(x_2 - t))f = 0$, which shows that 1 is a telescoper for f.

Section 5.5

1. In the second paragraph of the section, we argued that a nonzero solution of the linear system must lead to a nonzero telescoper because $D_x \cdot \frac{b_0+\cdots+b_s x^s}{q^r}$ is only zero if $b_0 = \cdots = b_s = 0$. This is only true because $\frac{b_0+\cdots+b_s x^s}{q^r}$ cannot be a nonzero constant, and this is because the degree condition $\deg_x(p) < \deg_x(q) - 1$ in combination with the choice $s = \deg_x(p) + (r - 1)\deg_x(q) + 1$ implies that the numerator of $\frac{b_0+\cdots+b_s x^s}{q^r}$ has a smaller degree than its denominator.

In order to enforce a nonzero telescoper in the case $\deg_x(p) \geq \deg_x(q) - 1$, we have to adjust the ansatz for the certificate to ensure that it does not become a nonzero constant. This can be done by omitting the term $b_{r \deg_x(q)} x^{r \deg_x(q)}$ from the ansatz. With the same choice $s = \deg_x(p) + (r - 1)\deg_x(q) + 1$ we then have only $(r + 1) + (s + 1 - 1)$ variables but still $\deg_x(p) + r \deg_x(q) + 1$ equations, which confirms the claim that there are telescopers of order r for every $r \geq \deg_x(q) - 1$.

For the degree bound, we make an ansatz over C with a certificate of the form

$$\frac{1}{q^r} \sum_{i=0\ i\neq r\deg_x(q)}^{s} \ \sum_{j=0}^{d+\deg_t(p)\ +(r-1)\deg_t(q)} b_{i,j} x^i t^j.$$

The modified ansatz has fewer variables but the same number of equations. With r and d chosen as in the theorem, we have more variables than equations and therefore a nontrivial solution.

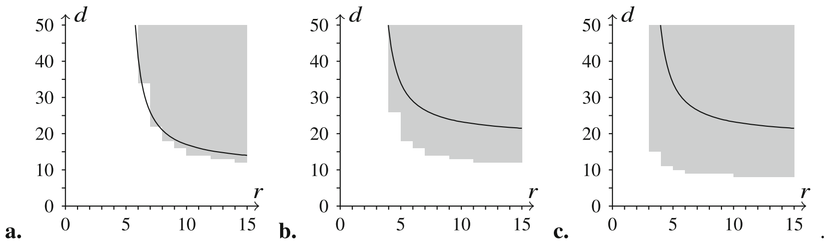
2. We get n more variables but also n more equations. As the bound on r emerges from the difference of variables and equations, n cancels out and the resulting bound is not affected at all.

3. First note that $D_t^r \cdot (\frac{p}{q}) = \frac{(\cdots)}{q(q^*)^r}$ with a numerator of x-degree at most $\deg_x(p) + r\deg_x(q^*)$. For the certificate, take an ansatz of the form $\frac{1}{q(q^*)^{r-1}} \sum_{i=0}^{s} b_i x^i$ with $s = \deg_x(p) + (r-1)\deg_x(q^*) + 1$. The linear system resulting from equating coefficients then has $(r+1) + (s+1) = r + \deg_x(p) + (r-1)\deg_x(q^*) + 3$ variables and $\deg_x(p) + r\deg_x(q^*) + 1$ equations, and it has a nonzero solution as soon as $r > \deg_x(q^*) - 2$. The justification that a nonzero solution implies a nonzero telescoper (Exercise 1) is not affected.

4. **a.** $\frac{1}{2}w(2d - w + 1) + (r + 1 - w)(d + 1)$; **b.** $(\deg_x(p) + r\deg_x(q) + 1)(d - w + \deg_t(p) + r\deg_t(q) + 1)$, because the t-degree of $q^{r+1}P \cdot (\frac{p}{q})$ with P being the proposed ansatz is the maximum of $(d - w + i) + \deg_t(p) + r\deg_t(q) - i = d - w + \deg_t(p) + r\deg_t(q)$ for $i = 0, \dots, w-1$ and $d + \deg_t(p) + r\deg_t(q) - i \le d - w + \deg_t(p) + r\deg_t(q)$ for $i \ge w$; **c.** $q^{-r}\sum_{i=0}^{s_1}\sum_{j=0}^{s_2} b_{i,j}x^i t^j$ with $s_1 = \deg_x(p) + (r-1)\deg_x(q) + 1$ and $s_2 = d - w + \deg_t(p) + (r-1)\deg_t(q)$; **d.** There is a telescoper for every (r, d) with $r > \alpha$ and $d > \frac{\beta r + \tilde{\gamma}}{r - \alpha}$, where α, β are as in Theorem 5.51 and $\tilde{\gamma} = \gamma + \frac{1}{2}w(w + 3 - 2\deg_x(q))$, with the γ from Theorem 5.51; **e.** $\frac{1}{2}w(w+3-2\deg_x(q))$ assumes its minimum at $w = \deg_x(p) - \frac{3}{2}$, the closest integer values are $\deg_x(p) - 1$ and $\deg_x(p) - 2$. By symmetry of the quadratic parabola, it does not matter which one we choose. Both choices lead to the improved bound $\tilde{\gamma} = \gamma - \frac{1}{2}(\deg_x(q) - 1)(\deg_x(q) - 2)$.

5. The arithmetic size of the denominator q^r is $(r\deg_x(q) + 1)(r\deg_t(q) + 1)$ if we expand it, and $(\deg_x(q) + 1)(\deg_t(q) + 1)$ if we keep it factored. The arithmetic size of the numerator is bounded $(\deg_x(p) + (r-1)\deg_x(q) + 1)(d + \deg_t(p) + (r-2)\deg_t(q))$. Observe that the certificate is much bigger than the telescoper.

6.



7. The telescoper of order 1 and degree 3 annihilates $(-1)^n\binom{4n}{n}$, and since $\sum_k (-1)^k\binom{n}{k}\binom{4n+k}{2n}$ is a sum with natural boundaries and equals $(-1)^n\binom{4n}{n}$, every telescoper of the summand must annihilate $(-1)^n\binom{4n}{n}$. It is therefore sufficient to show that $(-1)^n\binom{4n}{n}$ has no annihilating operator of degree less than 3. To see this, consider the algorithms for finding hypergeometric solutions of a given recurrence presented in Sect. 2.6. Because of $(-1)^{n+1}\binom{4(n+1)}{n+1}/(-1)^n\binom{4n}{n} = -\frac{8(2n+1)(4n+1)(4n+3)}{3(n+1)(3n+1)(3n+2)}$ and $\gcd(8(2(x+i)+1)(4(x+i)+1)(4(x+i)+3), 3(x +$

$1)(3x+1)(3x+2)) = 1$ for all $i \in \mathbb{Z}$, it follows that the leading and the trailing coefficient of any linear recurrence which has $(-1)^n\binom{4n}{n}$ among its hypergeometric solutions must have degree 3.

8. **a.** Suppose that $T_1, T_2 \in C[n][S_n]$ are two telescopers of the required shape, and let $T = \operatorname{gcrd}(T_1, T_2)$ (computed in $C(n)[S_n]$). As the telescopers of h form a left ideal in $C(n)[S_n]$, it follows that T is a telescoper, and by the assumption on $r_{\min}$, it follows that there are nonzero rational functions $q_1, q_2 \in C(n)$ such that $T = q_1T_1 = q_2T_2$. In particular, $T_1 = \frac{q_2}{q_1}T_2$. As T_1 and T_2 have polynomial coefficients of the same degree, the numerator of $\frac{q_2}{q_1}$ must have the same degree as its denominator. Their degrees must in fact be zero, because the minimality of $d_{\min}$ forces that the polynomial coefficients of T_2 are coprime (implying that the denominator of $\frac{q_2}{q_1}$ must be constant) and that the coefficients of T_1 are coprime (implying that the numerator of $\frac{q_2}{q_1}$ must be constant. **b.** No. For example, $k(k+1)(k+2)(k+3)\binom{n}{k}^3$ has two C-linearly independent telescopers of order 4 and degree 4 but no telescoper of order 4 and degree 3.

9. **a.** $p = \sum_{i=0}^{s} c_i(bn+b'k)^{\overline{ib}}, q = 1, r = (bn+b'k)^{\overline{b'}}$; **b.** $p = \sum_{i=0}^{s} c_i(un+u'k+iu)^{\overline{(r-i)u}}, q = 1, r = (un+u'k+ru-u')^{\overline{u'}}$; **c.** $p = \sum_{i=0}^{s} c_i(vn+v'k+iv)^{\overline{(r-i)v}}$, $q = (vn+v'k+rv-v')^{\overline{v'}}, r = 1$.

10. If we execute Gosper's algorithm for a hypergeometric term h with $\frac{S_k \cdot h}{h} = \frac{\sigma_k(p)}{p}\frac{q}{\sigma_k(r)}$, where p, r, q do not satisfy the condition $\gcd(q, \sigma_k^i(r)) = 1$ for all $i \in \mathbb{N} \setminus \{0\}$, and if we find a solution, it will be correct. The condition is only needed to ensure that we do not overlook any solutions, i.e., that Gosper's algorithm is also correct in the case where it returns $\perp$. In the present situation, we are only interested in a bound on the order of the telescoper, so if we miss some solution, it only means that the bound overshoots.

11. Consider the term $f_\alpha = k\Gamma(n+\alpha k)$. Clearly, the bitsize of f_α depends only logarithmically on α. We show that the order of the minimal telescoper of f_α is at least $\alpha - 1$. Applying Gosper's algorithm to $P \cdot f_\alpha$ for some $P = c_0 + \cdots + c_s S_n^s$ with undetermined $c_0, \ldots, c_s$ leads to the Gosper equation $\sum_{i=0}^{s} c_i k(n+\alpha k)^{\overline{i}} = (n+\alpha k)^{\overline{\alpha}}\sigma_k(y) - y$. If $c_s \neq 0$, then the left hand side is a polynomial in k of degree $s+1$, and this degree must be matched by the right hand side, whose degree in k is $\alpha + \deg_k(y)$ for $\alpha > 0$. Note that a cancellation among the summands can only happen if $\alpha = 0$. Now $s+1 = \alpha + \deg_k(y)$ together with $\deg_k(y) \geq 0$ implies $s \geq \alpha - 1$.

12. For any polynomial p, Theorem 5.53 predicts a telescoper of order r for the term $h = p\Gamma(n+rk)$. According to Exercise 11 in Sect. 5.4, we can choose p such that h is summable, i.e., such that h has a telescoper of order zero.

13. For example, every univariate rational function $\frac{p}{q} \in C(x) \subseteq C(x,t)$ has D_t as telescoper. It is not even necessary that q is squarefree.

14. $r \approx \alpha + \beta - 1 - 2\sqrt{(\alpha-1)\beta + \gamma}, d \approx \beta - \sqrt{(\alpha-1)\beta+\gamma}$.

15. **a.** We show by induction on i that the coefficients of $q^{i+1} D_t^i \cdot (\frac{p}{q})$ are bounded by $M^{i+1}(\deg_t(p) + i\deg_t(q))^i$. The claimed bound follows from this. For $i = 0$ we have $q^{i+1} D_t^i \cdot (\frac{p}{q}) = p$ and the bound is M by assumption. For the induction step $i \to i+1$, we have the assumption that $D_t^i \cdot (\frac{p}{q}) = \frac{u}{q^{i+1}}$ for some polynomial u whose coefficients are bounded by $b := M^{i+1}(\deg_t(p) + i\deg_t(q))^i$. We know also that $\deg_t(u) \le \deg_t(p) + i\deg_t(q)$. Therefore, $D_t^{i+1} \cdot (\frac{p}{q}) = \frac{u'q - uq'}{q^{i+2}}$, and the coefficients of $u'q - uq'$ are bounded by $bM\deg_t(u) + bM\deg_t(q) \le M^{i+1}(\deg_t(p) + i\deg_t(q))^i M(\deg_t(p) + (i+1)\deg_t(q)) \le M^{i+2}(\deg_t(p) + (i+1)\deg_t(q))$, as required. **b.** We have a linear system with $n := (\deg_x(p) + r\deg_x(q) + 1)(d + \deg_t(p) + r\deg_t(q) + 1)$ equations and a number of variables that is at least one more than that. The entries of the linear system are bounded in absolute value by $M^{r+1}(\deg_t(p) + r\deg_t(q))^r$. (In fact, the entries in the columns corresponding to the certificate part are smaller.) In view of Cramer's rule, the size of the coordinates of a solution vector can be estimated in terms of the determinant of the matrix. Using Hadamard's bound, we obtain the bound $\left(M^{r+1}(\deg_t(p) + r\deg_t(q))^r\sqrt{n}\right)^n$ for the integers in the telescoper.

16. $(an + a'k + a'')^{\overline{ia}}$ is a product of ia polynomials, the ℓth of which has coefficients bounded by $\Omega + \ell$ ($\ell = 0, \dots, ia - 1$). It follows from the definition of polynomial multiplication that the height of the product of some polynomials is bounded by the product of the heights of the factors. Therefore, the height of $(an + a'k + a'')^{\overline{ia}}$ is bounded by $\prod_{\ell=0}^{ia-1}(\Omega + \ell) = \Omega^{\overline{ia}}$.

17. Write $p = p_0 + \cdots + p_d x^d$ with $p_0, \dots, p_d \in \mathbb{Z}$ and $p_d \neq 0$. Then $p(\xi) = 0$ implies $|p_d\xi^d| = |-\sum_{i=0}^{d-1} p_i\xi^i|$ and $|p_d\xi^d| \ge |\xi|^d$ together with $|-\sum_{i=0}^{d-1} p_i\xi^i| \le \sum_{i=0}^{d-1}|p_i||\xi^i| \le \sum_{i=0}^{d}|p_i||\xi|^{d-1} \le \|p\|_\infty|\xi|^{d-1}$ implies the result.

18. Writing $P = \sum_{i=0}^{r}\sum_{j=0}^{d} p_{i,j}x^j D^i$, the indicial polynomial of P as defined in Definition 3.34 is $\eta = \sum_{i=0}^{r} p_{i,d+i-k}x^{\underline{i}} \in C[x]$, where k is the largest integer that yields a nonzero η. The coefficients of $x^{\underline{i}}$ are bounded by $i!$, the coefficients of $p_{i,d+i-k}x^{\underline{i}}$ are thus bounded by $Mi!$, so finally the coefficients of η are bounded by $M\sum_{i=0}^{r} i! \le 2Mr!$. As explained in Sect. 3.4, the starting exponent e of any power series solution $x^e + \cdots \in \mathbb{Q}[x]$ of P must be a root of η. Therefore, the claim follows from the previous exercise.

19. Consider the factorization $p = p_1^{e_1}\cdots p_k^{e_k}$ of p into pairwise distinct monic irreducible factors. Because of $p \mid q$, the factorization of q has the form $p = p_1^{f_1}\cdots p_k^{f_k} p_{k+1}^{f_{k+1}}\cdots p_n^{f_n}$ for certain $f_1, \dots, f_n \in \mathbb{N}$ with $e_i \le f_i$ for $i = 1, \dots, k$. The choice $g = p_1^{f_1}\cdots p_k^{f_k}$ has the desired property. If we can factor polynomials, it is clear that g can be computed. If we want to avoid factorization, we can set $g = p$ and repeatedly set $g = g\gcd(g, q/g)$ until $\gcd(g, q/g) = 1$.

20. Like in the proof of Theorem 5.60, we show that in each iteration the value of i is strictly smaller than in the previous iteration. Consider the value of i in a certain iteration and write $b_{\text{old}}, b_{\text{new}}$ for the values of b at the beginning and at the end of this iteration, respectively. In line 13, b_{new} is obtained from b_{old} by removing all factors of g at the cost of possibly introducing some factors of $v\sigma_k(g)$. Factors of g cannot also appear in $\sigma_k(g)$, because if r were a nontrivial irreducible factor of both g and $\sigma_k(g)$, then it would be a common factor of $\sigma_k(b)$ and $\sigma_k^{-i}(u)$, so $\gcd(b, \sigma_k^{-(i+1)}(u)) \neq 1$, in contradiction to the maximality of i. Therefore, none of the factors of g which get removed from b_{old} can get reintroduced by $\sigma_k(g)$.

It is also not possible that there is a $j \geq i$ such that $\gcd(b_{\mathrm{new}}, \sigma_k^{-j}(u)) \neq 1$. To see this, consider an irreducible factor r of b_{new}. Then r is contained either in b_{old} or in $\sigma_k(g)$. If it is contained in b_{old}, it cannot be contained in $\sigma_k^{-j}(u)$, by the maximality of i and the definition of b_{new}. So suppose that r is contained in $\sigma_k(g)$. It then appears in $\sigma_k(b_{\mathrm{old}})$, so if it also a factor of $\sigma_k^{-j}(u)$, then it is in fact a common factor of $\sigma_k(b_{\mathrm{old}})$ and $\sigma_k^{-j}(u)$, which implies $\gcd(b_{\mathrm{old}}, \sigma_k^{-(j+1)}(u)) \neq 1$, again in contradiction to the maximality of i.

21. With $s = \frac{2k(3k+2)}{(2k+1)(2k+3)(k+1)}$ and $f_{\mathrm{ker}} = \binom{2k}{k}$ we have $\frac{u}{v} = \frac{2(2k+1)}{k+1}$. We enter the first loop of Algorithm 5.59 with $i = 1$ and set $g = 2k + 3$. We update $s = s - \frac{15}{2(2k+3)} + \frac{k}{2(2k-1)}\frac{15}{2(2k+1)} = -\frac{21k^2-13k-10}{4(k+1)(2k-1)(2k+1)}$ and set $w = \frac{15k}{4(2k-1)(2k+1)}$. Now $b = 4(2k + 1)$ and the first loop terminates. There is no work for the second loop. In line 14 we get $p_1 = \frac{7}{4}$, $p_2 = \frac{15}{8}$, $p_3 = -2$, so we update $s = s + \frac{15}{8(k+1)} - \frac{15}{16(2k-1)} = \frac{7}{16(2k+1)} - \frac{1}{8(k+1)}$ and $w = w - \frac{15}{16(2k-1)} = \frac{15}{16(2k+1)}$. The final result is $\frac{2k(3k+2)}{(2k+1)(2k+3)(k+1)}\binom{2k}{k} = \Delta_k \cdot (\frac{7}{16(2k+1)} - \frac{1}{8(k+1)})\binom{2k}{k} + \frac{15}{16(2k+1)}\binom{2k}{k}$.

22. Let $w = \frac{p}{q} \in C(x)$ be such that $g = wh_{\mathrm{ker}}$, so that $h = g'$ translates into $\frac{a}{b} + \frac{c}{v} = w' + \frac{u}{v}w$. Then $av + cb = bvw' + buw$. Since the left hand side is a polynomial, so must the right hand side be. We show that q must be a constant.

Suppose otherwise and let q_0 be an irreducible factor of q. Then q_0 appears in the denominator of w' with higher multiplicity than in q, so it must be contained in v in order to enable the required cancellation. If it appeared in v with multiplicity larger than 1, then the multiplicity of q_0 in the denominator of w would exceed that in bvw', so u would have to contain q_0 as well, which cannot be because h_{ker} is a kernel. So the multiplicity of q_0 in v is 1. Moreover, if e is the multiplicity of q_0 in q, the calculation $vw' + uw = v^{-(e-1)}(v^e w' + ev^{e-1}v'w) - ev'w + uw = v^{-(e-1)}(v^e w)' + (u - ev')w$ shows that q_0 must be a divisor of $u - ev'$, because it appears in the denominator of $v^{-(e-1)}(v^e w)'$ with multiplicity $e - 1$ but in the denominator of w with multiplicity e. We have thus found that q_0 divides $\gcd(v, u - ev')$, but since h_{ker} is a kernel, $\gcd(v, u - ev') = 1$.

This completes the argument that q is a constant. So w is a polynomial and the right hand side of $av + cb = bvw' + buw$ is a polynomial which contains b as divisor. Then $b \mid av + cb$, then $b \mid av$, and finally $b \mid a$, because $\gcd(b, v) = 1$.

23. **a.** $\frac{\sigma_k(h/v)}{h/v} = \frac{\sigma_k(h)}{h}\frac{v}{\sigma_k(v)} = \frac{u}{v}\frac{v}{\sigma_k(v)} = \frac{u}{\sigma_k(v)}$. By assumption, h is a kernel, so we have $\gcd(u, \sigma_k^i(v)) = 1$ for all $i \in \mathbb{Z}$. We then also have $\gcd(u, \sigma_k^i(\sigma_k(v))) = 1$ for all $i \in \mathbb{Z}$. **b.** The conditions $\gcd(b, \sigma_k^{-i}) = \gcd(b, \sigma_k^{i+1}(b)) = 1$ for all $i \in \mathbb{N}$ are not affected, and the condition $\gcd(b, \sigma_k^i(v)) = 1$ for all $i \in \mathbb{N}$ gets replaced by the weaker condition $\gcd(b, \sigma_k^i(\sigma_k(v))) = 1$ for all $i \in \mathbb{N}$.

24. Theorem 5.62 is based on a summability obstruction rooted in the shell of the hypergeometric term. For a hypergeometric term which is a kernel, b in Theorem 5.62 will be constant and there are no irreducible factors p of b that could justify a nontrivial lower bound on the order of the telescoper. The bound will therefore be zero. On the other hand, note that all hypergeometric terms considered in Example 5.65 are kernels, and we have seen there that the minimal telescoper can have arbitrarily large order. So for any given r, the term $f_\alpha(n, k)$ with $\alpha = r$ is an example with the requested property. A simpler family serving the same purpose appears in the solution to Exercise 11.

25. **a.** Here we can use creative telescoping. The first sum has the telescoper $S_n + 1$ with the certificate $\frac{n-k}{k-n-1}$. For the second sum, we have the telescoper 1 with the certificate $\frac{k-\ell}{n-\ell}$. **b.** If we write p in the binomial basis, $p = c_0\binom{x}{0} + c_1\binom{x}{1} + \cdots$, the first part implies that $\sum_k (-1)^k \binom{n}{k} p(n) = (-1)^n c_n$. It remains to show that $c_n = n![x^n]p$. This follows readily from $\binom{x}{n} = \frac{1}{n!}x^n + \cdots$. **c.** View $\binom{mk}{n}$ as a polynomial in k of degree n, observe that its leading coefficient is $\frac{1}{n!}m^n$, and apply the formula from the previous part.

Section 5.6

1. Let $f_1, f_2 \in C(x)$ and let $g_1, g_2, h_1, h_2 \in C(x)$ be such that for $i = 1, 2$, $f_i = g_i' + h_i$, h_i has a squarefree denominator, and the denominator degree exceeds the numerator degree. For any $\alpha_1, \alpha_2 \in C$, we clearly have $\alpha_1 f_1 + \alpha_2 f_2 = (\alpha_1 g_1 + \alpha_2 g_2)' + (\alpha_1 h_1 + \alpha_2 h_2)$, and $\alpha_1 h_1 + \alpha_2 h_2$ is a rational function with a squarefree denominator whose degree exceeds the degree of the numerator. It remains to show that $\alpha_1 h_1 + \alpha_2 h_2$ must be the output of Algorithm 5.1 for the input $\alpha_1 f_1 + \alpha_2 f_2$. Let $h \in C(x)$ be the output and let $g \in C(x)$ be such that $\alpha_1 f_1 + \alpha_2 f_2 = g' + h$. Then $0 = (\alpha_1 g_1 + \alpha_2 g_2 - g)' + (\alpha_1 h_1 + \alpha_2 h_2 - h)$, so $\alpha_1 h_1 + \alpha_2 h_2 - h$ is integrable. The denominator of a sum of rational functions with squarefree denominators must also be squarefree. In view of Theorem 5.2, an integrable rational function with a squarefree denominator is zero. Therefore $h = \alpha_1 h_1 + \alpha_2 h_2$, as claimed.

2. **a.** False. For example, $R = \mathrm{id}\colon C^2 \to C^2$ is a reduction with respect to the subspace U generated by $\binom{1}{0}$ and we have $R^2 = R$, but $\ker R = \{0\} \neq U$, so R is not complete. **b.** True. $v - R(v) \in U = \ker R$ implies $R(v - R(v)) = R(v) - R^2(v) = 0$, so $R^2(v) = R(v)$ for all $v \in V$. **c.** False. For example, id is a reduction for every U because $v - \mathrm{id}(v) = 0 \in U$ and $\ker \mathrm{id} = \{0\} \subseteq U$, but $2\,\mathrm{id}$ is not a reduction for any $U \neq V$, because $v - 2\,\mathrm{id}(v) = -v \notin U$ for any $v \notin U$. **d.** False. For example, take $R_1 = R_2 = \mathrm{id}$ so that $R_1 + R_2 = 2\,\mathrm{id}$. **e.** True if R is a complete reduction, because then $v \in \ker R \cap \mathrm{im}\, R$ means $R(v) = 0$ and $v = R(w)$ for some w, so $R^2(w) = 0$, so $R(w) = 0$ by part a, so $v = R(w) = 0$. If R is not complete, the assertion is false. For example, take $V = C^2$ and $R = v \mapsto \binom{1\ 1}{0\ 1}v$, which is a reduction for $U = V$.

3. It follows from Exercise 1 that R is a reduction for U. The reduction is not confined because, for example, $R(\frac{x_2^n}{(1+x_1x_2)^2}) = \frac{nx_2^{n-1}}{x_1(1+x_1x_2)}$ for all $n \in \mathbb{N}$. It is also not complete because, for example, $R(\frac{x_1+x_2+x_1x_2}{(1+x_2)(x_1+x_2)^2}) = -\frac{1}{(x_1-1)(x_2+1)(x_1+x_2)} \neq 0$ while $\frac{x_1+x_2+x_1x_2}{(1+x_2)(x_1+x_2)^2} = (D_{x_1} \cdot \frac{x_1}{(x_1+x_2)(1+x_2)}) + (D_{x_2} \cdot \frac{x_2}{x_1+x_2})$.

4. a. True. By linearity, it suffices to consider the case when p is a monomial, say $p = x_1^{e_1} \cdots x_n^{e_n}$. Then $\sum_{i=1}^n x_i(D_{x_i} \cdot p) = \sum_{i=1}^n x_i e_i x_1^{e_1} \cdots x_n^{e_n}/x_i = \sum_{i=1}^n e_i p = dp$, as required. **b.** True. Every polynomial p can be written uniquely as $p = p_0 + \cdots + p_m$, where each p_j is a homogeneous polynomial of degree j. By part a, $\sum_{i=1}^n x_i(D_{x_i} \cdot p) = \sum_{i=1}^n x_i(D_{x_i} \cdot \sum_{j=0}^m p_j) = \sum_{j=0}^m jp_j$. In order for this to be equal to $dp = \sum_{j=0}^m dp_j$ for some d, we must have $p = p_d$, so p must be homogeneous. **c.** True. Using part a, we can calculate $\sum_{i=1}^n x_i(D_{x_i} \cdot \frac{p}{q}) = \sum_{i=1}^n x_i \frac{(D_{x_i} \cdot p)q - p(D_{x_i} \cdot q)}{q^2} = \frac{1}{q}\deg(p)p - \frac{p}{q^2}\deg(q)q = (\deg(p) - \deg(q))\frac{p}{q}$. **d.** True. From $d\frac{p}{q} = \sum_{i=1}^n x_i(D_{x_i} \cdot \frac{p}{q}) = \frac{1}{q}\sum_{i=1}^n x_i(D_{x_i} \cdot p) - \frac{p}{q^2}\sum_{i=1}^n x_i(D_{x_i} \cdot q)$ we have $dpd = q\sum_{i=1}^n x_i(D_{x_i} \cdot p) - q\sum_{i=1}^n x_i(D_{x_i} \cdot q)$, so $q \mid \sum_{i=1}^n x_i(D_{x_i} \cdot q)$, because p and q are coprime. As the degrees on both sides agree, it follows that $q = c\sum_{i=1}^n x_i(D_{x_i} \cdot q)$ for some constant c, and by part b, this implies that q is homogeneous and $c = \deg(q)$. We can then continue the above calculation $d\frac{p}{q} = \cdots = \frac{1}{q}\sum_{i=1}^n x_i(D_{x_i} \cdot p) - \deg(q)\frac{p}{q}$, which implies $(d - \deg(q))p = \sum_{i=1}^n x_i(D_{x_i} \cdot p)$. Again using part b, it follows that p is homogeneous and $d - \deg(q) = \deg(p)$.

5. Let $k \in \mathbb{N}$ and let $p, q \in C[x_1, \ldots, x_n]$ be homogeneous polynomials of respective degrees r, s. We have $\sum_{i=1}^n D_{x_i} \cdot \frac{x_i p}{q^k} = \sum_{i=1}^n \frac{(D_{x_i} \cdot x_i)pq + x_i(D_{x_i} \cdot p)q - kx_i p(D_{x_i} \cdot q)}{q^{k+1}} = \frac{p}{q^k}\sum_{i=1}^n 1 + \frac{1}{q^k}\sum_{i=1}^n x_i(D_{x_i} \cdot p) - k\frac{p}{q^{k+1}}\sum_{i=1}^n x_i(D_{x_i} \cdot q) = n\frac{p}{q^k} + r\frac{p}{q^k} - ks\frac{p}{q^k} = (n + r - ks)\frac{p}{q^k}$, so $\frac{p}{q^k} = \frac{1}{n+r-ks}\sum_{i=1}^n D_{x_i} \cdot \frac{x_i p}{q^k}$ unless $n + r - ks = 0$.

6. a. The equation is equivalent to $p = \sum_{i=1}^n b_i(D_{x_i} \cdot q) + (\sum_{i=1}^n (D_{x_i} \cdot b_i) + c)$. By assumption, $p \in \langle D_{x_1} \cdot q, \cdots, D_{x_n} \cdot q\rangle$, so there are $b_1, \ldots, b_n \in C[x_1, \ldots, x_n]$ with $p = \sum_{i=1}^n b_i(D_{x_i} \cdot q)$. For any such choice of $b_1, \ldots, b_n$ we can set $c = -\sum_{i=1}^n (D_{x_i} \cdot b_i)$ and obtain a solution. **b.** Nearly any choice works. For example, take $p = 1$, $q = x^2 + y^2$, $k = 2$. The equation then simplifies to $1 = -2xb_1 - 2yb_2 + (x^2 + y^2)((D_x \cdot b_1) + (D_y \cdot b_2) + c)$, which does not have a polynomial solution because every term appearing on the right hand side is a multiple of x or a multiple of y, so the right hand side has no chance to be equal to 1.

7. Consider $f = \frac{1}{((xy)^2+1)^2}$. We have $I = \langle xy\rangle$ and can take $G = \{xy\}$. In line 4 of Algorithm 5.71, we then have $u = \mathrm{red}(1, G) = 1$. A possible choice for b_1, b_2 is $b_1 = b_2 = 0$, and with this choice the algorithm returns $\frac{1}{((xy)^2+1)^2}$. Another possible choice is $b_1 = x$, $b_2 = -x$. With this choice, we get $h_0 = \frac{1}{2((xy)^2+1)}$ in line 5, so the final output is $\frac{1}{((xy)^2+1)^2} + \frac{1}{2((xy)^2+1)}$.

8. No. For $f = \frac{1}{(x^2+1)^2}$ we have $I = \langle x \rangle$ and can take $G = \{x\}$. Then $u = \operatorname{red}(1, G) = 1$, so Algorithm 5.71 returns $\frac{1}{(x^2+1)^2}$ unchanged. Hermite reduction finds the decomposition $f = \big(\frac{x}{2(x^2+1)}\big)' + \frac{1}{2(x^2+1)}$.

9. **a.** $(7t^2 + 6t - 9)(4t^3 - 27)D_t^2 + 2(77t^4 + 78t^3 - 135t^2 + 189t + 81)D_t + 4(t+3)(14t^2 - 27t - 9)$; **b.** $t(27t-4)(3t^3 + 18t^2 - 5t - 2)D_t^2 + 2(81t^4 + 732t^3 - 288t^2 - 120t + 10)D_t + 6(3t^3 + 44t^2 - 20t - 40)$; **c.** $9t^2 D_t^2 + 36t D_t + 8$.

10. We have $D_t^i \cdot f = \frac{(-1)^i i!}{(t+x^3+x^2y)^{i+1}}$ for every $i \in \mathbb{N}$. For $q = t + x^3 + x^2 y$ we have $I = \langle D_x \cdot q, D_y \cdot q \rangle = \langle x^2, xy \rangle \subseteq C(t)[x, y]$, and $G = \{x^2, xy\}$ is a Gröbner basis regardless of the choice of the term order. Therefore, $\operatorname{red}((-1)^i i!, G) = (-1)^i i!$ for all $i \in \mathbb{N}$, so the application of Algorithm 5.71 to $D_t^i \cdot f$ yields $\frac{(-1)^i i!}{(t+x^3+x^2y)^{i+1}}$ for every $i \in \mathbb{N}$. As these rational functions are $C(t)$-linearly independent, the algorithm never finds a telescoper. Observe that we have $\dim_{C(t)} C(t)[x, y]/I = \infty$ in this example.

11. **a.** We show by induction on d that every $p \in C[k]$ of degree d can be uniquely written as a linear combination of elements of B. Note first that any linear combination $\lambda_0 b_0 + \cdots + \lambda_n b_n$ of some polynomials $b_i \in C[k]$ with $\deg_k(b_i) = i$ has degree n if $\lambda_n \neq 0$, because $b_0, \ldots, b_{n-1}$ have lower degree and cannot cancel the term $\lambda_n k^n$. It follows for $d = 0$ that we can and must write any $p \in C[k]$ as a constant multiple of the unique element of B whose degree is 0. Now let $d > 0$ and suppose that the claim holds for all degrees less than d. Let $p \in C[k]$ be of degree d. Then there is a unique $b \in C[k]$ of degree d and a unique $c \in C$ such that $\deg_k(p - cb) < d$, and by the induction hypothesis, $p - cb$ can be written uniquely as a linear combination of elements of B. The same is thus true for p. **b.** If $\deg_k(u) \neq \deg_k(v)$ or $\operatorname{lc}_k(u) \neq \operatorname{lc}_k(v)$ then $\deg_k(\varphi(y)) = \deg_k(y) + \max\{\deg_k(u), \deg_k(v)\}$ for every $y \in C[k]$. Therefore, we can choose $d = \max\{\deg_k(u), \deg_k(v)\}$ in this case. If $\deg_k(u) = \deg_k(v)$ and $\operatorname{lc}_k(u) = \operatorname{lc}_k(v)$, then write $\varphi(y) = u\Delta_k(y) - (v - u)y$. For any polynomial $y = k^i + \cdots$ we then have $\varphi(y) = (\operatorname{lc}_k(u)i - (\operatorname{lc}_k(v) - \operatorname{lc}_k(u)))k^{\deg_k(u)+i-1} + \cdots$, so $\deg_k(\varphi(y)) = \deg_k(u) + \deg_k(y) - 1$ or $i = \frac{\operatorname{lc}_k(v)}{\operatorname{lc}_k(u)} - 1$. In the latter case, we can still say that $\deg_k(\varphi(y)) < \deg_k(u) + \frac{\operatorname{lc}_k(v)}{\operatorname{lc}_k(u)} - 1$. Therefore, we can choose $d = \deg_k(u) + \max\{-1, \frac{\operatorname{lc}_k(v)}{\operatorname{lc}_k(u)} - 1\}$. **c.** Use Algorithm 2.56 to compute the vector space of all $(y, c_0, \ldots, c_{d-1}) \in C[k] \times C^d$ such that $u\sigma_k(y) - vy = c_0 + c_1 k + \cdots + c_{d-1} y^{d-1}$. Drop the first component to obtain a subspace U of C^d, and use linear algebra to find a $V \subseteq C^d$ with $U \oplus V = C^d$. Then we can take $W = \{c_0 + \cdots + c_{d-1}k^{d-1} : (c_0, \ldots, c_{d-1}) \in V\}$.

12. $h - \tilde{h}$ is summable, so $f - \tilde{f}$ is summable, so according to Theorem 5.77, $h - \tilde{h}$ should be zero, but it isn't.

13. For $u = 1$ and $v = (an+bk)\cdots(an+bk+b-1)$, the image of $\varphi\colon C(n)[k] \to C(n)[k]$ defined by $\varphi(y) = u\sigma_k(y) - vy$ contains polynomials of any degree $d \geq b$. For a linear subspace $W \subseteq C(n)[k]$ with $C(n)[k] = \operatorname{im}\varphi \oplus W$ we therefore have $\dim_C W \leq b$. For every $i \in \mathbb{N}$, we have $f = S_n^i \cdot \Gamma(an+bk) = \Gamma(an+bk+ai) = (an+bk)^{\overline{ia}} f_{\mathrm{ker}} = (\frac{(an+bk)^{\overline{ia}}}{1} + \frac{0}{v}) f_{\mathrm{ker}} = (\frac{0}{1} + \frac{v(an+bk)^{\overline{ia}}}{v}) f_{\mathrm{ker}}$. So, for every such f, the corresponding h belongs to the $C(n)$-vector space $\frac{1}{v} f_{\mathrm{ker}} W$. Since its dimension is bounded by b, the h's corresponding to $f_{\mathrm{ker}}, S_n \cdot f_{\mathrm{ker}}, \ldots, S_n^b \cdot f_{\mathrm{ker}}$ are $C(n)$-linearly dependent. Hence f_{ker} has a telescoper of order at most b.

14. We have $R(S_n^i \cdot f) = (\frac{a_i}{k+n+7} + \frac{c_i}{k+1})\binom{n}{k}$ for

$$a_0 = -\frac{8(2n+1)(2n+3)(2n+5)(2n+7)}{n(n+4)(n+5)(n+6)}, \quad c_0 = \frac{43n^6+410n^5+1637n^4+3406n^3+3960n^2+2424n+720}{n(n+2)(n+3)(n+4)(n+5)(n+6)},$$

$$a_1 = \frac{4(2n+3)(2n+5)(2n+7)}{(n+4)(n+5)(n+6)}, \quad c_1 = -\frac{2(n-1)(5n^4+46n^3+167n^2+276n+180)}{(n+2)(n+3)(n+4)(n+5)(n+6)},$$

$$a_2 = -\frac{2(n+1)(2n+5)(2n+7)}{(n+4)(n+5)(n+6)}, \quad c_2 = \frac{2(n+1)(2n^4+22n^3+109n^2+269n+270)}{(n+2)(n+3)(n+4)(n+5)(n+6)}.$$

The resulting telescoper does not change.

15. The results remain the same.

16. Algorithm 5.76 replaces $(\frac{1}{1} + \frac{0}{v}) f_{\mathrm{ker}}$ by $(\frac{0}{1} + \frac{v}{v}) f_{\mathrm{ker}}$ and then works on the numerator of $\frac{v}{v}$. It remains unchanged if and only if $v \in W$, so the question is whether this can happen. We can choose a W with $v \in W$ unless $v \in \operatorname{im}\varphi$, so the question is whether we always have $v \in \operatorname{im}\varphi$. This is certainly not the case. Take for example $f_{\mathrm{ker}} = k!$ so that $u = k+1$ and $v = 1$. Then $\operatorname{im}\varphi$ only contains polynomials with positive degree (apart from 0), so it cannot contain v.

17. **a.** There are six cases to distinguish: $a \leq b \leq c$, $a \leq c \leq b$, $b \leq a \leq c$, $b \leq c \leq a$, $c \leq a \leq b$, $c \leq b \leq a$. The first case is too boring. Let's discuss the second. The others work similarly. For $a \leq c \leq b$, we have $\sum\nolimits'^{\,b}_{k=a} u_k + \sum\nolimits'^{\,c}_{k=b+1} u_k = \sum_{k=a}^{b} u_k - \sum_{k=c+1}^{b+1-1} u_k = \sum_{k=a}^{c} u_k$. **b.** For $b \geq 0$ we have $\sum\nolimits'^{\,b}_{k=0} q^k = \sum_{k=0}^{b} q^k = \frac{1-q^{b+1}}{1-q}$. For $b < 0$ we have $\sum\nolimits'^{\,b}_{k=0} q^k = -\sum_{k=b+1}^{-1} q^k = -\frac{q^{b+1}-q^{-1+1}}{1-q} = \frac{1-q^{b+1}}{1-q}$, so $\sum\nolimits'^{\,b}_{k=0} q^k = \frac{1-q^{b+1}}{1-q}$ for all $b \in \mathbb{Z}$. By part a, $\sum\nolimits'^{\,b}_{k=a} q^k = \sum\nolimits'^{\,-1}_{k=a} q^k + \sum\nolimits'^{\,b}_{k=0} q^k = \sum\nolimits'^{\,b}_{k=0} q^k - \sum\nolimits'^{\,a-1}_{k=0} q^k = \frac{1-q^{b+1}}{1-q} - \frac{1-q^a}{1-q} = \frac{q^a-q^{b+1}}{1-q}$ for all $a, b \in \mathbb{Z}$.

18. We follow the structure of the inductive definition of binomial sums. For $(\delta_n)_{n\in\mathbb{Z}}$ we can take $q = 1$. For a geometric sequence $((\frac{u}{v})^n)_{n\in\mathbb{Z}}$ we can take $q = \operatorname{lcm}(u, v)$. For the binomial coefficient sequence we can take $q = 1$. For the sum and the product of two binomial sums, we can take the product of the corresponding q's. For the affine map and the directed sum, we can take as q the q of the original sequence.

19. We have $|\binom{n}{k}| \leq 2^{|n|+|k|}$ for all $n, k \in \mathbb{Z}$ and $|\delta_{n,0}| \leq 1$ and $|q^n| = |q|^n$ for all $n \in \mathbb{Z}$ and all $q \in \mathbb{Q}$. Moreover, linear combinations and products of sequences bounded by exponential terms are bounded by exponential terms. A change of variables applied to a sequence with at most exponential growth yields a sequence with at most exponential growth. Finally, $|\sum_{k=0}^{n} q^k| \leq (1+|q|)^n$. Altogether, it follows that for every binomial sum $(a_{n_1,\dots,n_d})_{n_1,\dots,n_d\in\mathbb{N}}$ there exist $c, q \in \mathbb{Q}$ such that $|a_{n_1,\dots,n_d}| \leq cq^{n_1+\cdots+n_d}$ for all $n_1,\dots,n_d \in \mathbb{N}$. As no such c and q exist for $a_n = n!$, this sequence cannot be a binomial sum.

20. **a.** $\sum_{n=0}^{\infty} a_n t^n = \operatorname{Res}_{x_1,x_2,x_3}\big(x_1x_2x_3(1-x_1)(1-x_2(x_3+1))(1-t\frac{1+\frac{x_1}{x_3}}{x_1x_2})\big)^{-1}$; **b.** $\sum_{n=0}^{\infty} b_n t^n = \operatorname{Res}_{x_1,x_2}\big(x_1x_2(1-x_1)(1-2x_2)(1-\frac{t}{x_1}-\frac{x_1}{x_2})\big)^{-1}$; **c.** $\sum_{n=0}^{\infty} c_n t^n = \operatorname{Res}_{x_1,x_2}\big(x_1x_2(1-x_1)(1-x_2^2)(1-t\frac{(\frac{x_1}{x_2}+1)^3}{x_1^2})\big)^{-1}$.

21. **a.** By the assumption on the term order, the smallest term of $1-x_1q$ is 1, regardless of the monomials appearing in q. Therefore, $\frac{p}{1-x_1q} = \operatorname{Res}_{x_1} p\sum_{n=0}^{\infty}(x_1q)^n$, and it is clear from here that the residue is zero. **b.** For example, for $p = x_n^{-1}$ and $q = 0$ we have $\operatorname{Res}_{x_n} p/(x_1-q) = \frac{1}{x_1} \neq 0$. **c.** If r is a Laurent polynomial in x_1, i.e., an element of $C(x_2,\dots,x_n)[x_1,x_1^{-1}]$, then its residue with respect to x_1 is just one of its coefficients, which is evidently an element of $C(x_2,\dots,x_n)$. If r is not a Laurent polynomial in x_1, there are $p, q \in C(x_2,\dots,x_n)[x_1]$ and $k \in \mathbb{Z}$ such that $r = x_1^k\frac{p}{1-x_1q} = x_1^k p\sum_{n=0}^{\infty}(x_1q)^n$ the residue of which is $\sum_{n=0}^{\infty}([x_1]^{-1-k-n}p)q^n$. This sum is finite because p is a polynomial in x_1. So the residue is rational. **d.** For example, we have $\operatorname{Res}_{x_2}\frac{1}{1-(x_2+x_2^{-1})x_1} = \frac{1-4x_1^2-\sqrt{1-4x_1^2}}{2x_1(2x_1-1)(2x_1+1)}$, which is clearly irrational.

22. Creative telescoping algorithms can find the annihilating operator $L = (t^2-34t+1)t^2D_t^3 + 3(2t^2-51t+1)tD_t^2 + (7t^2-112t+1)D_t + (t-5)$ for the right hand side. Using Zeilberger's algorithm, it is also not hard to compute the annihilating operator $(n+2)^3S_n^2 - (2n+3)(17n^2+51n+39)S_n + (n+1)^3$ for A_n. Using Theorem 2.33 we can translate this operator into a differential operator of order 5 which annihilates $\sum_{n=0}^{\infty} A_n t^n$, and which turns out to be a left multiple of L. The claimed identity is thus proven by comparing a few initial terms. The rational function in this exercise appears in [95].

Software

Implementations of the algorithms presented in this book are available for various computer algebra systems. We won't give a comprehensive introduction to using these tools but only a minimalistic list of examples intended as quick reference. Readers are referred to the documentation of the packages for further information. Note that some of the packages mentioned below do not belong to the standard distributions but have to be installed separately.

Mathematica

Guessing Using the Guess package by Kauers [262], univariate recurrences, differential equations, or algebraic equations can be found as follows:

In[1]:= **<< Guess.m**
Guess Package by Manuel Kauers — V 0.59 n-15

In[2]:= **GuessMinRE[{1, 3, 13, 63, 321, 1683, 8989, 48639, 265729}, *f*[*n*]]**

Out[2]= $(1 + n) f[n] + (-9 - 6n) f[1 + n] + (2 + n) f[2 + n]$

In[3]:= **GuessMinDE[{1, 3, 13, 63, 321, 1683, 8989, 48639, 265729}, *f*[*x*]]**

Out[3]= $(-3 + x) f[x] + (1 - 6x + x^2) f'[x]$

In[4]:= **GuessMinAE[{1, 3, 13, 63, 321, 1683, 8989, 48639, 265729}, *f*[*x*]]**

Out[4]= $-1 + (1 - 6x + x^2) f[x]^2$

The method for multivariate sequences takes as input a bound on the order and a bound on the degree. The shape of the sought equation can be specified more accurately through options.

In[5]:= ***data* = Table[Binomial[*n*, *k*]Binomial[*n* + *k*, *k*], {*n*, 0, 10}, {*k*, 0, 10}];**

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1

In[6]:= **GuessMultRE[*data*, $f[n,k]$, 1, 1]**

Out[6]= $\{(-k-n-1)f(n,k)+(\frac{n}{2}+\frac{1}{2})f(n,k+1)+(k-\frac{n}{2}+\frac{1}{2})f(n+1,k+1),\ (k+n+1)f(n,k)+(k-n-1)f(n+1,k),\ (k+n+1)f(n,k)+(k+\frac{n}{2}+\frac{3}{2})f(n,k+1)+(-\frac{n}{2}-\frac{1}{2})f(n+1,k+1)\}$

Closure properties can be executed using Koutschan's package HolonomicFunctions.m [291]. This package provides a data type for Ore polynomials. D-finite functions are represented by bases of D-finite ideals of annihilating operators. There is a powerful command for transforming a symbolic expression into such a representation.

In[7]:= **<< HolonomicFunctions.m**
HolonomicFunctions package by Christoph Koutschan, RISC-Linz, Version 1.6 (12.04.2012)

In[8]:= **Annihilator[Binomial[2n, n]^{2}LegendreP[n, x], {S[n], Der[x]}]**

Out[8]= $\{(1+2n+n^2)S_n+(2+4n-2x^2-4nx^2)D_x+(-2x-6nx-4n^2x),\ (-1+x^2)D_x^2+2xD_x+(-n-n^2)\}$

The command uses algorithms for closure properties behind the scenes. There are also commands for accessing these algorithms directly. For example, the least common left multiple and the symmetric product of two operators can be computed as follows.

In[9]:= **DFinitePlus[{ToOrePolynomial[S[n] − n]}, {ToOrePolynomial[S[n]^2 − S[n] − 1]}]**

Out[9]= $\{(-1+n^2)S_n^3+(1-3n^2-n^3)S_n^2+(1+n^2+n^3)S_n+(2n^2+n^3)\}$

In[10]:= **DFiniteTimes[{ToOrePolynomial[S[n] − n]}, {ToOrePolynomial[S[n]^2 − S[n] − 1]}]**

Out[10]= $\{S_n^2+(-1-n)S_n+(-n-n^2)\}$

Similar commands are available for further closure properties. They all work also in the multivariate case.

Koutschan's package also provides a command for finding *rational solutions* of coupled systems of linear recurrence equations or differential equations.

In[11]:= **SolveCoupledSystem[{$xf'[x] - f[x] + g[x] + c_0x, x(x+1)g'[x] + 2f[x] + c_1$}, {$f, g$}, {$x$},
ExtraParameters → {c_0, c_1}]**

Out[11]= $\{\{f[x]\to\dfrac{C[1]+xC[2]}{x},\ c_0\to 0,\ c_1\to 2(C[1]-C[2]),\ g[x]\to\dfrac{2C[1]+xC[2]}{x}\}\}$

D'Alembertian solutions can be found with Schneider's package Sigma [392], generalized series solutions of recurrences with Kauers's package Asymptotics [263].

Koutschan's package has various commands for *creative telescoping*. The standard command takes as input a D-finite annihilating ideal of operators or an expression specifying the summand/integrand, the operator corresponding to the summation/integration variable (typically S[k] − 1 for summation or Der[x] for integration), and a list of generators of the algebra in which the resulting telescopers live. Its output consists of a pair of lists, the first list containing telescopers and the second list the corresponding certificates.

In[12]:= **CreativeTelescoping[Binomial[n, k]Binomial[$n+k$, k], S[k] − 1, {S[n]}]**

Out[12]= $\{\{(2+n)S_n^2 + (-9-6n)S_n + (1+n)\}, \{\frac{2k^2(3+2n)}{2-3k+k^2+3n-2kn+n^2}\}\}$

In[13]:= **CreativeTelescoping[Binomial[n, k]LegendreP[k, x]^2, Der[x], {S[n], S[k]}]**

Out[13]= $\{\{(3+5k+2k^2)S_k + (k+2k^2-n-2kn), (-1+k-n)S_n + (1+n)\},$
$\{\frac{k-n-kx^2+nx^2}{1+k}D_x - (1+k)xS_k + (-(kx)+nx), 0\}\}$

Sage

In Sage, functionality for D-finite functions is available via the ore_algebra package by Kauers, Jaroschek, Johansson, and Mezzarobba [267, 277]. Its command for guessing takes as input an array of terms and an algebra indicating the kind of annihilating operators that should be guessed.

```
sage: from ore_algebra import *
sage: guess([1, 3, 13, 63, 321, 1683, 8989,
        48639, 265729], OreAlgebra(ZZ['n'], 'Sn'))
```

$(-n-2)S_n^2 + (6n+9)S_n - n - 1$

```
sage: guess([1, 3, 13, 63, 321, 1683, 8989,
        48639, 265729], OreAlgebra(ZZ['x'], 'Dx'))
```

$(-t^2+6t-1)D_t - t + 3$

```
sage: data = [[binomial(n, k)*binomial(n+k, k)
        for k in range(20)] for n in range(20)];
sage: guess(data, OreAlgebra(ZZ['n','k'],'Sn','Sk'),
        order=1, degree=1).groebner_basis()
```

$[(k^2+2k+1)S_k - n^2 + k^2 - n + k, (n-k+1)S_n - n - k - 1]$

Closure properties in the univariate case are available as methods attached to operator objects. In the multivariate case, they are available in left ideal objects.

```
sage: x = ZZ['x'].gen()
sage: Dx = OreAlgebra(ZZ[x], 'Dx').gen()
sage: (Dx + 1).lclm(x*Dx - 1)
```

$(x+1)D_x^2 + xD_x - 1$

```
sage: (Dx + 1).symmetric_product(x*Dx - 1)
```

$xD_x + x - 1$

```
sage: x, y = ZZ['x', 'y'].gens()
sage: R.<Dx, Dy> = OreAlgebra(ZZ[x, y])
sage: R.ideal([(x + y)*Dx - 1, (x + y)*Dy - 1])
        .intersection(R.ideal([Dx, Dy]))
```

Left Ideal $(D_x - D_y, D_y^2)$ of Multivariate Ore algebra in D_x, D_y over Fraction Field of Multivariate Polynomial Ring in x, y over Integer Ring

Univariate operators also contain methods for finding rational and other kinds of solutions.

```
sage: n = ZZ['n'].gen()
sage: R.<Sn> = OreAlgebra(ZZ[n])
sage: ((3 + n + 3*n^2) + (7 + 7*n + 3*n^2)*Sn
        - (34 + 26*n + 6*n^2)*Sn^2
        - (66 + 38*n + 6*n^2)*Sn^3
        + (55 + 25*n + 3*n^2)*Sn^4
        + (83 + 31*n + 3*n^2)*Sn^5)
        .rational_solutions()
```

$[(\frac{1}{3n^2+n+3},), (\frac{n}{3n^2+n+3},)]$

```
sage: (Sn^3 - 1).rational_solutions([1, n^3])
```

$[(1, 0, 0), (n, 3, 0), (n^4 - 6n^3 + 9n^2, 0, 12)]$

An implementation of creative telescoping is available in left ideal objects.

```
sage: n, k = ZZ['n', 'k'].gens()
sage: R.<Sn,Sk> = OreAlgebra(ZZ[n,k])
sage: R.ideal([(1 + 2*k + k^2)*Sk + (k + k^2 - n - n^2),
        (-1 + k - n)*Sn + (1 + k + n)]).ct(Sk - 1)
```

$([(-n-2)S_n^2 + (6n+9)S_n - n - 1], [\frac{4nk^2+6k^2}{n^2-2nk+k^2+3n-3k+2}])$

Maple

Guessing and univariate closure properties are available in the classical Maple package gfun by Salvy and Zimmermann [379].

```
> with(gfun):
> data:=[1, 3, 13, 63, 321, 1683, 8989, 48639, 265729]:
> listtorec(data, f(n));
```

$$[\{(-n-3)\,\mathrm{f}(n+3) + (15+6n)\,\mathrm{f}(n+2) + (-2-n)\,\mathrm{f}(n+1), \mathrm{f}(0) = 1, \mathrm{f}(1) = 3, \mathrm{f}(2) = 13\}, ogf]$$

```
> listtodiffeq(data, f(x));
```

$$[\{(-x^2+6x-1)\left(\frac{d}{dx}\,\mathrm{f}(x)\right)+(-x+3)\,\mathrm{f}(x),\mathrm{f}(0)=1\},ogf]$$

```
> listtoalgeq(data, f(x));
```

$$[1+(-x^2+6x-1)\,\mathrm{f}(x)^2,ogf]$$

```
> `diffeq+diffeq`(diff(f(x),x)-f(x),
        x*diff(f(x),x)-f(x),f(x));
```

$$\mathrm{f}(x)-x\left(\frac{d}{dx}\,\mathrm{f}(x)\right)+(-1+x)\left(\frac{d^2}{dx^2}\,\mathrm{f}(x)\right)$$

```
> `diffeq*diffeq`(diff(f(x),x)-f(x),
        x*diff(f(x),x)-f(x),f(x));
```

$$(-x-1)\,\mathrm{f}(x)+x\left(\frac{d}{dx}\,\mathrm{f}(x)\right)$$

The Mgfun package by Chyzak [154] covers the multivariate case.

```
> with(Mgfun):
> `sys+sys`({(x + y)*diff(f(x, y), x) - f(x, y),
        (x + y)*diff(f(x, y), y) - f(x, y)},
        {diff(f(x, y), x), diff(f(x, y), y)});
```

$$\{-\left(\frac{d}{dx}\,\mathrm{f}(x,y)\right)+\left(\frac{d}{dy}\,\mathrm{f}(x,y)\right),\frac{d^2}{dx^2}\,\mathrm{f}(x,y)\}$$

Some closure properties for the univariate case are also available in the packages DETools (differential case) and LRETools (shift case). These packages contains a lot of additional functionality, including methods for factoring operators and for finding rational and other kinds of solutions.

```
> with(DETools):
> LCLM(x *Dx - 1, Dx - 1, [x, Dx]);
```

$$Dx^2-\frac{xDx}{-1+x}+\frac{1}{-1+x}$$

```
> DFactorLCLM(%, [Dx, x]);
```

$$[Dx-1/x,Dx-1]$$

```
> DFactor(%%, [Dx, x]);
```

$$[Dx-\frac{1}{-1+x},Dx-1]$$

```
> symmetric_product(x*Dx - 1, Dx - 1, [x, Dx]);
```

$$xDx-x-1$$

```
> ratsols((x^2 - 1)*diff(f(x),x,x)
        - (5 - x^2)*diff(f(x),x)
        - 4*f(x), f(x));
```

$$\left[\frac{x+3}{-1+x}\right]$$

```
> with(LRETools):
> ratpolysols((x + 1)*f(x + 1) - x *f(x), f(x), {});
```

$$\frac{\_C[0]}{x}$$

There are several implementations of creative telescoping for hypergeometric summands or hyperexponential integrands. An implementation for general D-finite input is available in the Mgfun package.

```
> Mgfun[creative_telescoping](binomial(n, k)*binomial
        (n+k, k),
        n::shift, k::shift);
```

$$[[(n+1)\,\_\mathrm{F}(n) + (n+1)\,\_\mathrm{F}(n+2) + (-6n-9)\,\_\mathrm{F}(n+2), -\frac{2(2n+3)k^2\,\_\mathrm{f}(n,k)}{(-n+k-1)(-n+k-2)}]]$$

```
> sumtools[sumrecursion](binomial(n, k)*binomial
        (n + k, k), k, f(n));
```

$$(n-1)\,\mathrm{f}(n-2) - 3(2n-1)\,\mathrm{f}(n-1) + \mathrm{f}(n)n$$

```
> SumTools[Hypergeometric][MinimalTelescoper]
        (binomial(n, k) *binomial (n + k, k), k, Sn);
```

$$(-n-2)Sn^2 + (6n+9)Sn - 1 - n$$

```
> DETools[Zeilberger](x/(1 - 2*x *y - y^3), x, y, Dx);
```

$$[54 + (32x^5 + 27x^2)Dx^2 + (80x^4 - 54x)Dx, \frac{4x^3(10xy^4 + 12x^2y^2 - 16xy + 9)}{(y^3+2xy-1)^2}]$$

Notation

$f: A \to B$	f is a function from A to B	1
$(a_n)_{n=0}^{\infty}$, $(a_n)_{n\in\mathbb{Z}}$	Notation for sequences with index sets $\mathbb{N}$ and $\mathbb{Z}$, respectively	1
B^A	Set of all functions $f: A \to B$	1
$B[[x]]$	Ring of formal power series with coefficients in B.	2
$[x^n]f$	Coefficient of x^n in f	2
$B[[x^{-1}]]$	Ring of formal power series with coefficients in B and descending powers of x	2
$B((x))$	Ring of formal Laurent series	2
$\operatorname{ord}(f)$, $\nu(f)$	Order or valuation of the series f	2
$B[x]$	Ring of polynomials in x with coefficients in B	3
$\deg(p)$, $\deg_x(p)$	Degree of the polynomial $p \in B[x]$	3
$B[x, x^{-1}]$	Ring of Laurent polynomials in x with coefficients in B	3
C	An arbitrary field of characteristic zero	4
$C(x)$	Field of rational functions in x with coefficients in C	4
a', a'', a''', $a^{(i)}$	First, second, third, and ith derivative of a	7
$u^{\overline{n}}$	nth rising factorial of u	11
${}_pF_q\left(\begin{matrix}\alpha_1, \dots, \alpha_p \\ \beta_1, \dots, \beta_q\end{matrix} \,\middle\vert\, x\right)$	Traditional notation for a hypergeometric series	11
$\binom{\alpha}{n}$	Binomial coefficient	13
$u^{\underline{n}}$	nth falling factorial of u	13
$V(f)$	Vector space generated by f and its derivatives/shifts over $C(x)$	18
$\dim_C V$	Dimension of V as vector space over C	18

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1

$[f]$	Equivalence class of f	21
$D, D_x, D_y, \ldots$	Standard symbols used for the derivation operator	21
$L \cdot f$	Result of applying the operator L to f	21
$S, S_x, S_n, \ldots$	Standard symbols used for the shift operator	21
$C(x)[\partial]$	Algebra of linear operators with coefficients in $C(x)$	22
$\mathrm{O}(g(n))$	Big-O notation for asymptotic estimates ($n \to \infty$)	36
$\mathrm{O}^{\sim}(g(n))$	Soft-O notation for asymptotic estimates ($n \to \infty$)	37
$\mathrm{M}_{\mathbb{Z}}(n)$	Integer multiplication time	37
$\mathrm{quo}_{\mathbb{Z}}(a, b), \mathrm{rem}_{\mathbb{Z}}(a, b)$	Quotient and remainder for integers	38
$b \mid a$	b divides a	38
$\gcd_{\mathbb{Z}}(a, b)$	Greatest common divisor of the integers a, b	38
$\mathbb{Z}_m$	Residue class ring mod m	38
$\mathrm{lc}(p)$	Leading coefficient of the polynomial p	42
$\mathrm{M}(n)$	Polynomial multiplication time	42
$\mathrm{quo}(a, b), \mathrm{rem}(a, b)$	Quotient and remainder for polynomials	43
$\gcd(a, b)$	Greatest common divisor of the polynomials a, b	43
$C[x]/\langle m \rangle$	Quotient of $C[x]$ by the ideal $\langle m \rangle$ generated by $m \in C[x]$	44
$\nu_q(r)$	Valuation/multiplicity of $r \in C(x)$ with respect to $q \in C[x]$	46
ω	Matrix multiplication exponent	48
$\deg^{\delta} p$	Relative degree of a vector of polynomials	73
$\mathrm{ord}_f\, p$	Order of a vector p of polynomials with respect to a vector f of power series	73
$\mathrm{Const}(R)$	Constant ring of R	104
χ	Standard variable for the characteristic polynomial	128
η	Standard variable for the indicial polynomial	128
$C[[[x]]]$	Ring of generalized series	131
$\Delta, \Delta_x, \Delta_n$	Forward difference operator	133
$\mathrm{Spread}(a, b)$	Spread of $a, b \in C[x]$	153
$\mathrm{Disp}(a, b)$	Dispersion of $a, b \in C[x]$	153
$T_{\zeta_1 \to \zeta_2}$	Transition matrix	192
$\mathrm{ord}(L)$	Order of the operator L	291
$\mathrm{lc}(L)$	Leading coefficient of the operator L	291
$\mathrm{lt}(L)$	Leading term of the operator L	291
$\langle L_1, \ldots, L_m \rangle$	(Left) Ideal generated by $L_1, \ldots, L_m$	292
$\mathrm{ann}(f)$	Annihilator of f	293
$V(L)$	Solution space of L	293
$L \otimes M$	Symmetric product of L and M	297

$L^{\otimes n}$	nth symmetric power L	297
$L \oplus M$	Symmetric sum of L and M	297
$\sigma^{\overline{m}}(p)$	$= p\sigma(p)\cdots\sigma^{m-1}(p)$	300
$\mathrm{rquo}(U, V)$	Right quotient of U by V	304
$\mathrm{rrem}(U, V)$	Right remainder of U by V	304
$\mathrm{gcrd}(U, V)$	Greatest common right divisor	305
$\mathrm{lclm}(U, V)$	Least common left multiple	305
$\mathrm{Syl}(U, V)$	Sylvester matrix of U and V	308
$\mathrm{res}(U, V)$	Resultant of U and V	308
$P[A]$	Gauge transformation of A by P	330
P^*	Adjoint of the operator P	344
E_L	Eigenring of the operator L	346
$W(y_1, \ldots, y_r)$	Wronskian of $y_1, \ldots, y_r$	349
$\bigwedge^s V$	Exterior power of V	353
$v_1 \wedge \cdots \wedge v_s$	Element of an exterior power	353
$\mathrm{sgn}(\pi)$	Sign of a permutation π	353
$R[\partial_1, \ldots, \partial_n]$	Multivariate Ore algebra	361
$\mathrm{lt}(p)$	Leading term of p (in the multivariate case)	378
$\mathrm{lc}(p)$	Leading coefficient of p (in the multivariate case)	378
$\mathrm{lm}(p)$	Leading monomial of p, i.e., $\mathrm{lm}(p) = \mathrm{lc}(p)\,\mathrm{lt}(p)$	378
$\mathrm{lexp}(p)$	Exponent vector of the leading term of p	378
$\mathrm{red}(p, G)$	A reduced form of p with respect to G as computed by Algorithm 4.76	379
$\mathrm{spol}(p, q)$	S-polynomial of p and q	382
$\mathrm{Syz}(b_1, \ldots, b_m)$	Syzygy module of $b_1, \ldots, b_m$	387
$\mathrm{Res}_{x-\alpha} h$	Residue of h at $x = \alpha$	396
$\binom{n}{k}_q$	q-binomial coefficient	410
$C_{\mathbb{Z}}[[x_1, \ldots, x_n]]$	Series in $x_1, \ldots, x_n$ with unrestricted support	437
$\mathrm{Res}_{x_1,\ldots,x_n} f$	Residue of the series f w.r.t. $x_1, \ldots, x_n$	437
$C_{\leq}((x_1, \ldots, x_n))$	Formal Laurent series field in several variables	439
$\mathrm{diag}\, f$	Diagonal of a formal power series	439
$[x^{>}]f$	Positive part of the series f	439
$f \odot_{x_1,\ldots,x_n} g$	Hadamard product of f and g w.r.t. the variables $x_1, \ldots, x_n$.	440
$\langle f \| g \rangle$	Scalar product of symmetric functions	445
$f * g$	Internal product of symmetric functions	445
$\\|p\\|_\infty$	Largest absolute value of the coefficients of the polynomial p	474
${\sum'}_{k=a}^{b} u_k$	directed sum	501

References

1. Abdelaziz, Y., Koutschan, C., Maillard, J.-M.: On Christol's conjecture. J. Phys. A **53**(20), 205201 (2020)
2. Abramov, S.A.: On the summation of rational functions. Zh. vychisl. Mat. Fiz 1071–1075 (1971)
3. Abramov, S.A.: Rational solutions of linear differential and difference equations with polynomial coefficients. USSR Comput. Math. Math. Phys. **29**(6), 7–12 (1989)
4. Abramov, S.A.: Rational solutions of linear difference and q-difference equations with polynomial coefficients. In: Proceedings of the ISSAC'95, pp. 285–289 (1995)
5. Abramov, S.A.: m-sparse solutions of linear ordinary differential equations with polynomial coefficients. Discrete Math. **217**(1–2), 3–15 (2000)
6. Abramov, S.A.: Applicability of Zeilberger's algorithm to hypergeometric terms. In: Proceedings of the ISSAC'02, pp. 1–7 (2002)
7. Abramov, S.A.: When does Zeilberger's algorithm succeed? Adv. Appl. Math. **30**(3), 424–441 (2003)
8. Abramov, S.A., Barkatou, M.A.: Rational solutions of first order linear difference systems. In: Proceedings of the ISSAC'98, pp. 124–131 (1998)
9. Abramov, S.A., van Hoeij, M.: Desingularization of linear difference operators with polynomial coefficients. In: Proceedings of the ISSAC'99, pp. 269–275 (1999)
10. Abramov, S.A., van Hoeij, M.: Integration of solutions of linear functional equations. Integral Transforms Spec. Funct. **8**, 3–12 (1999)
11. Abramov, S.A., van Hoeij, M.: Set of poles of solutions of linear difference equations with polynomial coefficients. Comput. Math. Math. Phys. **43**(1), 57–62 (2003)
12. Abramov, S.A., Kvashenko, K.Y.: Fast algorithms to search for the rational solutions of linear differential equations with polynomial coefficients. In: Proceedings of the ISSAC'91, pp. 267–270 (1991)
13. Abramov, S.A., Le, H.Q.: A criterion for the applicability of Zeilberger's algorithm to a rational function. Discrete Math. **259**(1–3), 1–17 (2002)
14. Abramov, S.A., Le, H.Q.: On the order of the recurrence produced by the method of creative telescoping. Discrete Math. **298**(1–3), 2–17 (2005)
15. Abramov, S.A., Petkovšek, M.: D'Alembertian solutions of linear differential and difference equations. In: Proceedings of the ISSAC'94, pp. 169–174 (1994)
16. Abramov, S.A., Petkovšek, M.: Proof of a conjecture of Wilf and Zeilberger. Technical Report 39/748, Institute of Mathematics, Physics, and Mechanics, 2001
17. Abramov, S.A., Petkovšek, M.: Minimal decomposition of indefinite hypergeometric sums. In: Proceedings of the ISSAC'01, pp. 7–14 (2001)

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1

18. Abramov, S.A., Petkovšek, M.: On the structure of multivariate hypergeometric terms. Adv. Appl. Math. **29**(3), 386–411 (2002)
19. Abramov, S.A., Petkovšsek, M.: Dimensions of solution spaces of h-systems. J. Symb. Comput. **43**(5), 377–394 (2008)
20. Abramov, S.A., Zima, E.V.: A universal program to uncouple linear systems. In: Proceedings of the CMCP'96, vol. 7, pp. 16–21 (1997)
21. Abramov, S.A., Bronstein, M., Petkovšek, M.: On polynomial solutions of linear operator equations. In: Proceedings of the ISSAC'95, pp. 290–296 (1995)
22. Abramov, S.A., Paule, P., Petkovšek, M.: q-hypergeometric solutions of q-difference equations. Discrete Math. **180**, 3–22 (1998)
23. Abramov, S.A., Le, H.Q., Li, Z.: Univariate Ore polynomial rings in computer algebra. J. Math. Sci. **131**, 5885–5903 (2005)
24. Abramov, S.A., Barkatou, M.A., van Hoeij, M.: Apparent singularities of linear difference equations with polynomial coefficients. Applicable Algebra Eng. Commun. Comput. **17**(2), 117–133 (2006)
25. Abramov, S.A., Barkatou, M.A., van Hoeij, M., Petkovšek, M.: Subanalytic solutions of linear difference equations and multidimensional hypergeometric sequences. J. Symb. Comput. **46**(11), 1205–1228 (2011)
26. Abramov, S.A., Bronstein, M., Petkovšek, M., Schneider, C.: On rational and hypergeometric solutions of linear ordinary difference equations in $\Pi\Sigma^*$-field extensions. J. Symb. Comput. **107**, 23–66 (2021)
27. Abramowitz, M., Stegun, I.A.: Handbook of Mathematical Functions, 9th edn. Dover Publications, Mineloa (1972)
28. Adams, C.R.: On the irregular case of the linear ordinary difference equation. Trans. AMS **30**, 507–541 (1928)
29. Adams, W., Loustaunau, P.: An Introduction to Gröbner Bases. Graduate Studies in Mathematics, vol. 3. AMS, Providence (1994)
30. Almkvist, G., Zeilberger, D.: The method of differentiating under the integral sign. J. Symb. Comput. **11**(6), 571–591 (1990)
31. Anderson, F.W., Fuller, K.R.: Rings and Categories of Modules. Springer, Berlin (1992)
32. Andrews, G.E., Askey, R., Roy, R.: Special Functions. Encyclopedia of Mathematics and its Applications, vol. 71. Cambridge University Press, Cambridge (1999)
33. Andrews, G.E., Paule, P., Riese, A.: MacMahon's partition analysis: the Omega package. Eur. J. Comb. **22**(7), 887–904 (2001)
34. Andrews, G.E., Paule, P., Riese, A.: MacMahon's partition analysis VI: a new reduction algorithm. Ann. Comb. **5**, 251–270 (2001)
35. Apagodu, M., Zeilberger, D.: Multi-variable Zeilberger and Almkvist-Zeilberger algorithms and the sharpening of Wilf-Zeilberger theory. Adv. Appl. Math. **37**(2), 139–152 (2006)
36. Aparicio Monforte, A., Kauers, M.: Formal Laurent series in several variables. Exp. Math. **31**(4), 350–367 (2013)
37. Apel, J., Lassner, W.: An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. J. Symb. Comput. **6**, 361–370 (1988)
38. Aroca, J.M., Cano, J., Feng, R., Gao, X.-S.: Algebraic general solutions of algebraic ODEs. In: Proceedings of the ISSAC'05, pp. 29–36 (2005)
39. Balser, W.: From Divergent Power Series to Analytic Functions. Lecture Notes in Mathematics, vol. 1582. Springer, Berlin (1994)
40. Balser, W.: Formal Power Series and Linear Systems of Meromorphic Ordinary Differential Equations. Springer, Berlin (2000)
41. Barkatou, M.A.: An algorithm for computing a companion block diagonal form for a system of linear differential equations. Appl. Algebra Eng. Commun. Comput. **4**, 185–195 (1993)
42. Barkatou, M.A.: On rational solutions of systems of linear differential equations. J. Symb. Comput. **28**(4), 547–567 (1999)
43. Barkatou, M.A., Jaroschek, M.: Desingularization of first order linear difference systems with rational function coefficients. In: Proceedings of the ISSAC'18, pp. 39–46 (2018)

44. Barkatou, M.A., Jaroschek, M.: Removing apparent singularities of linear difference systems. J. Symb. Comput. **102**, 86–107 (2021)
45. Barkatou, M.A., Maddah, S.S.: Removing apparent singularities of systems of linear differential equations with rational function coefficients. In: Proceedings of the ISSAC'15, pp. 53–60 (2015)
46. Beck, M., Robins, S.: Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra. Springer, Berlin (2007)
47. Becker, T., Weispfenning, V., Kredel, H.: Gröbner Bases. Springer, Berlin (1993)
48. Beckermann, B.: Zur Interpolation mit polynomialen Linearkombinationen beliebiger Funktionen. Ph.D Thesis, University of Hannover, 1990
49. Beckermann, B., Labahn, G.: A uniform approach for Hermite-Padé and simultaneous Padé approximants and their matrix generalizations. Numer. Algorithms **3**, 45–54 (1992)
50. Beckermann, B., Labahn, G.: A uniform approach for the fast computation of matrix-type Padé approximants. SIAM J. Matrix Anal. Appl. **15**(3), 804–823 (1994)
51. Beeler, M., Gosper, B., Schroeppel, R.: HAKMEM. Technical Report 239, MIT, 1972
52. Beke, E.: Die Irreducibilität der homogenen linearen Differentialgleichungen. Math. Ann. **45**, 278–294 (1894)
53. Benoit, A., Chyzak, F., Darrasse, A., Gerhold, S., Mezzarobba, M., Salvy, B.: The dynamic dictionary of mathematical functions (DDMF). In: Proceedings of the ICMS 2010. LNCS, vol. 6327, pp. 35–41. Springer, Berlin (2010)
54. Benoit, A., Bostan, A., van der Hoeven, J.: Quasi-optimal multiplication of linear differential operators. In: Proceedings of the FOCS12, pp. 524–530 (2012)
55. Bergeron, F., Plouffe, S.: Computing the generating function of a series given its first terms. Exp. Math. **1**(4), 307–312 (1992)
56. Bergman, G.M.: The diamond lemma for ring theory. Adv. Math. **29**(2), 178–218 (1978)
57. Bernardi, O., Bousquet-Mélou, M., Raschel, K.: Counting quadrant walks via Tutte's invariant method. Comb. Theory **1**, #3 (2021)
58. Bernstein, J.N.: Modules over a ring of differential operators. study of the fundamental solutions of equations with constant coefficients. Funct. Anal. Appl. **5**, 89–101 (1971)
59. Bernstein, D.J.: Fast multiplication and its applications. In: Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography. Cambridge University Press, Cambridge (2008)
60. Bertrand, D.: Un analogue différentiel de la théorie de Kummer. In: Approximations Diophantiennes et Nombres Transcendants / Diophantine Approximations and Transcendental Numbers, pp. 39–49. De Gruyter, Berlin (1992)
61. Beuchler, S., Pillwein, V., Zaglmayr, S.: Sparsity optimized high order finite element functions for h(div) on simplices. Numer. Math. **122**(2), 197–225 (2012)
62. Beuchler, S., Pillwein, V., Zaglmayr, S.: Sparsity optimized high order finite element functions for h(curl) on tetrahedra. Adv. Appl. Math. **50**, 749–769 (2013)
63. Beukers, F.: Some congruences for the Apéry numbers. J. Number Theory **21**, 141–155 (1985)
64. Bézivin, J.-P.: Sur une classe d'equations fonctionnelles non linéaires. Funkcialaj Ekvacioj **37**, 263–271 (1994)
65. Bini, D., Pan, D.: Polynomial and Matrix Computations. Birkhäuser, Basel (1994)
66. Birkhoff, G.D.: General theory of linear difference equations. Trans. AMS **12**, 243–284 (1911)
67. Birkhoff, G.D.: Formal theory of irregular difference equations. Acta Math. **54**, 205–246 (1930)
68. Birkhoff, G.D., Trjitzinsky, W.J.: Analytic theory of singular difference equations. Acta Math. **60**, 1–89 (1933)
69. Bjork, J.-E.: Rings of Differential Operators. North-Holland, Amsterdam (1979)
70. Bliss, G.A.: Algebraic Functions. AMS, Providence (1933)
71. Blümlein, J., Kauers, M., Klein, S., Schneider, C.: Determining the closed forms of the $O(a_s^3)$ anomalous dimension and Wilson coefficients from Mellin moments by means of computer algebra. Comput. Phys. Commun. **180**(11), 2143–2165 (2009)

72. Bona, M.: Combinatorics of Permutations, 3rd edn. Taylor and Francis, Milton Park (2022)
73. Bostan, A.: Algorithmique efficace pour des opérations de base en calcul formel. Ph.D Thesis, Ecole polytechnique, 2003
74. Bostan, A., Calcul Formel pur la Combinatoire de Marches. Habilitation à Diriger des Recherches (2017)
75. Bostan, A., Kauers, M.: Automatic classification of restricted lattice walks. In: Proceedings of the FPSAC'09, pp. 201–215 (2009)
76. Bostan, A., Kauers, M., with an appendix by van Hoeij, M.: The complete generating function for Gessel walks is algebraic. Proc. AMS **138**(9), 3063–3078 (2010)
77. Bostan, A., Mori, R.: A simple and fast algorithm for computing the N-th term of a linearly recurrent sequence. In: Proceedings of the SOSA'21, pp. 118–132 (2021)
78. Bostan, A., Yurkevich, S.: A hypergeometric proof that Iso is bijective. Proc. AMS **150**(5), 2131–2136 (2022)
79. Bostan, A., Yurkevich, S.: On a class of hypergeometric diagonals. Proc. AMS **150**(3), 1071–1087 (2022)
80. Bostan, A., Cluzeau, T., Salvy, B.: Fast algorithms for polynomial solutions of linear differential equations. In: Proceedings of the ISSAC'05, pp. 45–52 (2005)
81. Bostan, A., Chyzak, F., Cluzeau, T., Salvy, B.: Low complexity algorithms for linear recurrences. In: Proceedings of the ISSAC'06, pp. 31–38 (2006)
82. Bostan, A., Gaudry, P., Schost, É.: Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. SIAM J. Comput. **36**(6), 1777–1806 (2007)
83. Bostan, A., Chyzak, F., Salvy, B., Lecerf, G., Schost, É.: Differential equations for algebraic functions. In: Proceedings of the ISSAC'07, pp. 25–32 (2007)
84. Bostan, A., Chyzak, F., Le Roux, N.: Products of ordinary differential operators by evaluation and interpolation. In: Proceedings of the ISSAC'08, pp. 23–30 (2008)
85. Bostan, A., Boukraa, S., Guttmann, T., Hassani, S., Jensen, I., Maillard, J.-M., Zenine, N.: High order fuchsian equations for the square lattice Ising model: $\tilde{\chi}^{(5)}$. J. Phys. A Math. Theor. **42**(27), 275209 (2009)
86. Bostan, A., Chen, S., Chyzak, D., Li, Z.: Complexity of creative telescoping for bivariate rational functions. In: Proceedings of the ISSAC'10, pp. 203–210 (2010)
87. Bostan, A., Boukraa, S., Christol, S., Hassani, S., Maillard, J.-M.: Ising n-fold integrals as diagonals of rational functions and integrality of series expansions: integrality versus modularity. Technical Report 1211.6031, ArXiv, 2012
88. Bostan, A., Chyzak, F., Li, Z., Salvy, B.: Fast computation of common left multiples of linear ordinary differential operators. In: Proceedings of the ISSAC'12, pp. 99–106 (2012)
89. Bostan, A., Boukraa, S., Christol, G., Hassani, S., Maillard, J.-M.: Ising n-fold integrals as diagonals of rational functions and integrality of series expansions. J. Phys. A **46**(18), 185202 (2013)
90. Bostan, A., Chen, S., Chyzak, F., Li, Z., Xin, G.: Hermite reduction and creative telescoping for hyperexponential functions. In: Proceedings of the ISSAC'13, pp. 77–84 (2013)
91. Bostan, A., Lairez, P., Salvy, B.: Creative telescoping for rational functions using the Griffith-Dwork method. In: Proceedings of the ISSAC'13, pp. 93–100 (2013)
92. Bostan, A., Chyzak, F., de Panafieu, E.: Complexity estimates for two uncoupling algorithms. In: Proceedings of the ISSAC'13, pp. 85–92 (2013)
93. Bostan, A., Caruso, X., Schost, É.: A fast algorithm for computing the p-curvature. In: Proceedings of the ISSAC'15, pp. 69–76 (2015)
94. Bostan, A., Chyzak, F., van Hoeij, M., Kauers, M., Pech, L.: Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. Eur. J. Comb. **61**, 242–275 (2017)
95. Bostan, A., Lairez, P., Salvy, B.: Multiple binomial sums. J. Symb. Comput. **80**, 351–386 (2017)

96. Bostan, A., Chyzak, F., Giusti, M., Lebreton, R., Lecerf, G., Salvy, B., Schost, É.: Algorithmes Efficaces en Calcul Formel. Published by the authors (2018). https://hal.archives-ouvertes.fr/AECF/
97. Bostan, A., Chyzak, F., Lairez, P., Salvy, B.: Generalized Hermite reduction, creative telescoping and definite integration of D-finite functions. In: Proceedings of the ISSAC'18, pp. 95–102 (2018)
98. Bostan, A., Rivoal, T., Salvy, B.: Explicit degree bounds for right factors of linear differential operators. Bull. LMS **53**(1), 53–62 (2021)
99. Boucher, D., Ulmer, F.: Codes as modules over skew polynomial rings. In: Proceedings of the 12th IMA conference on Cryptography and Coding. LNCS, vol. 5921, pp. 38–55 (2009)
100. Boucher, D., Ulmer, F.: Coding with skew polynomial rings. J. Symb. Comput. **44**, 1644–1656 (2009)
101. Boucher, D., Geiselmann, W., Ulmer, F.: Skew cyclic codes. Appl. Algebra Eng. Commun. Comput. **18**, 379–389 (2007)
102. Boucher, D., Gaborit, P., Geiselmann, Ruatta, W.O., Ulmer, F.: Key exchange and encryption schemes based on non-commutative skew polynomials. In: Proceedings of the Post-Quantum Cryptography. LNCS, vol. 6061, pp. 126–141 (2010)
103. Boukraa, S., Guttmann, T., Hassani, S., Jensen, I., Maillard, J.-M.: Bernhard Nickel, and Nadjah Zenine. Experimental mathematics on the magnetic susceptibility of the square lattice Ising model. J. Phys. A Math. Theor. **41**(45), 1–51 (2008)
104. Boukraa, S., Hassani, S., Maillard, J.-M.: Holonomic functions of several complex variables and singularities of anisotropic Ising n-fold integrals. J. Phys. A Math. Theor. **45**(49), 494010 (2012)
105. Bousquet-Mélou, M., Mishna, M.: Walks with small steps in the quarter plane. Contemp. Math. **520**, 1–40 (2010)
106. Braaksma, B.L.J., Faber, B.F., Immink, G.K.: Summation of formal solutions of a class of linear difference equations. Pac. J. Math. **195**(1), 35–65 (2000)
107. Brak, R., Guttmann, A.J.: Algebraic approximants: a new method of series analysis. J. Phys. A **23**(24), L1331–L1337 (1990)
108. Brent, R.P., Kung, H.-T.: Fast algorithms for manipulating formal power series. J. ACM **25**(4), 581–595 (1978)
109. Brent, R., Zimmermann, R.: Modern Computer Arithmetic. Cambridge University Press, Cambridge (2011)
110. Bronstein, M.: Linear ordinary differential equations: breaking through the order 2 barrier. In: Proceedings of the ISSAC'92, pp. 42–48 (1992)
111. Bronstein, M.: On solutions of linear ordinary differential equations in their coefficient field. J. Symb. Comput. **13**(4), 413–439 (1992)
112. Bronstein, M.: An improved algorithm for factoring linear ordinary differential operators. In: Proceedings of the ISSAC'94, pp. 336–340 (1994)
113. Bronstein, M.: On solutions of linear ordinary difference equations in their coefficient field. J. Symb. Comput. **29**(6), 841–877 (2000)
114. Bronstein, M.: Symbolic Integration I. Algorithms and Computation in Mathematics, vol. 1, 2nd edn. Springer, Berlin (2005)
115. Bronstein, M., Petkovšek, M.: An introduction to pseudo-linear algebra. Theor. Comput. Sci. **157**(1), 3–33 (1996)
116. Bronstein, M., Mulders, T., Weil, J.-A.: On symmetric powers of differential equations. In: Proceedings of the ISSAC'97, pp. 156–163 (1997)
117. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Ph.D Thesis, Universität Innsbruck, 1965
118. Buchberger, B., Möller, H.M.: The construction of multivariate polynomials with preassigned zeros. In: Proceedings of the EUROCAM'82, pp. 24–31 (1982)
119. Burger, R., Heinle, A.: A new primitive for a Diffie-Hellman-like key exchange protocol based on multivariate Ore polynomials. Technical Report 1407.1270, ArXiv, 2014

120. Bürgisser, P., Clausen, M., Shokrollahi, M.A.: Algebraic Complexity Theory. Springer, Berlin (1997)
121. Calkin, N.J.: A curious binomial identity. Discrete Math. **131**(1–3), 335–337 (1994)
122. Cantor, D.G., Kaltofen, E.: On fast multiplication of polynomials over arbitrary algebras. Acta Inf. **28**(7), 693–701 (1991)
123. Caruso, X., Le Borgne, J.: A new faster algorithm for factoring skew polynomials over finite fields. J. Symb. Comput. **79**(2), 411–443 (2017)
124. Cha, Y.: Closed Form Solutions of Linear Difference Equations. Ph.D Thesis, Florida State University, 2010
125. Cha, Y., van Hoeij, M.: Liouvillean solutions of irreducible linear difference equations. In: Proceedings of the ISSAC'09, pp. 87–93 (2009)
126. Cha, Y., van Hoeij, M., Levy, G.: Solving recurrence relations using local invariants. In: Proceedings of the ISSAC'10, pp. 303–309 (2010)
127. Chen, S.: Stability problems in symbolic integration. In: Proceedings of the ISSAC'22, pp. 517–524 (2022)
128. Chen, S., Kauers, M.: Order-degree curves for hypergeometric creative telescoping. In: Proceedings of the ISSAC'12, pp. 122–129 (2012)
129. Chen, S., Kauers, M.: Trading order for degree in creative telescoping. J. Symb. Comput. **47**(8), 968–995 (2012)
130. Chen, S., Koutschan, C.: Proof of the Wilf-Zeilberger conjecture for mixed hypergeometric terms. J. Symb. Comput. **93**, 133–147 (2019)
131. Chen, S., Singer, M.F.: Residues and telescopers for bivariate rational functions. Adv. in Appl. Math. **49**(2), 111–133 (2012)
132. Chen, W.Y.C., Sun, L.H.: Extended Zeilberger's algorithm for identities on Bernoulli and Euler polynomials. J. Number Theory **129**(9), 2111–2132 (2009)
133. Chen, W.Y.C., Paule, P., Saad, H.L.: Converging to Gosper's algorithm. Adv. Appl. Math. **41**(3), 351–364 (2008)
134. Chen, W.Y.C., Hou, Q.-H., Jin, H.-T.: The Abel-Zeilberger algorithm. Electron. J. Comb. **18**(2), #P17 (2011)
135. Chen, S., Kauers, M., Singer, M.F.: Telescopers for rational and algebraic functions via residues. In: Proceedings of the ISSAC'12, pp. 130–137 (2012)
136. Chen, S., Jaroschek, M., Kauers, M., Singer, M.F.: Desingularization explains order-degree curves for Ore operators. In: Proceedings of the ISSAC'13, pp. 157–164 (2013)
137. Chen, S., Kauers, M., Koutschan, C.: A generalized Apagodu-Zeilberger algorithm. In: Proceedings of the ISSAC'14, pp. 107–114 (2014)
138. Chen, S., Huang, H., Kauers, M., Li, Z.: A modified Abramov-Petkovšek reduction and creative telescoping for hypergeometric terms. In: Proceedings of the ISSAC'15, pp. 117–124 (2015)
139. Chen, S., Chyzak, F., Feng, R., Fu, G., Li, Z.: On the existence of telescopers for mixed hypergeometric terms. J. Symb. Comput. **68**(1), 1–26 (2015)
140. Chen, S., Kauers, M., Koutschan, C.: Reduction-based creative telescoping for algebraic functions. In: Proceedings of the ISSAC'16, pp. 175–182 (2016)
141. Chen, S., Kauers, M., Singer, M.F.: Desingularization of Ore operators. J. Symb. Comput. **74**(5/6), 617–626 (2016)
142. Chen, W.Y.C., Hou, Q.-H., Zeilberger, D.: Automated discovery and proof of congruence theorems for partial sums of combinatorial sequences. J. Differ. Equ. Appl. **22**(6), 780–788 (2016)
143. Chen, S., van Hoeij, M., Kauers, M., Koutschan, C.: Reduction-based creative telescoping for fuchsian D-finite functions. J. Symb. Comput. **85**, 108–127 (2018)
144. Chen, S., Du, L., Kauers, M: Lazy Hermite reduction and creative telescoping for algebraic functions. In: Proceedings of the ISSAC'21, pp. 75–82 (2021)
145. Chen, S., Q.-H. Hou, Huang, H., Labahn, G., Wang, R.-H.: Constructing minimal telescopers for rational functions in three discrete variables. Adv. Appl. Math. **141**, 102389 (2022)

146. Chevalley, C.: Introduction to the Theory of Algebraic Functions of One Variable. AMS, Providence (1951)
147. Christol, G.: Diagonales de fractions rationnelles et équations de Picard-Fuchs. Technical Report 1, Study group on ultrametric analysis, 1985
148. Christol, G.: Fonctions hypergéométriques bornées. Technical Report tome 14, exp. 8, Groupe de travail d'analyse ultramétrique, 1986–1987
149. Christol, G.: Globally bounded solutions of differential equations. In: Analytic Number Theory 1988. LNM, vol. 1434, pp. 45–64. Springer, Berlin (1990)
150. Chudnovsky, D.V., Chudnovsky, G.V.: Computer algebra in the service of mathematical physics and number theory. In: Computers in Mathematics, pp. 109–232. M. Dekker, New York (1986)
151. Chudnovsky, D.V., Chudnovsky, G.V.: Approximations and complex multiplication according to Ramanujan. In: Ramanujan revisited, pp. 375–472 (1988)
152. Churchill, R.C., Kovacic, J.J.: Cyclic vectors. In: Proceedings of DART'02, pp. 191–218 (2002)
153. Chyzak, F.: Gröbner bases, symbolic summation and symbolic integration. In: Gröbner Bases and Applications, pp. 32–60. Cambridge University Press, Cambridge (1997)
154. Chyzak, F.: Fonctions holonomes en calcul formel. Ph.D Thesis, INRIA Rocquencourt, 1998
155. Chyzak, F.: An extension of Zeilberger's fast algorithm to general holonomic functions. Discrete Math. **217**, 115–134 (2000)
156. Chyzak, F.: The ABC of Creative Telescoping – Algorithms, Bounds, Complexity. Habilitation à diriger des recherches. University Paris-Sud 11, 2014
157. Chyzak, F., Salvy, B.: Non-commutative elimination in Ore algebras proves multivariate identities. J. Symb. Comput. **26**, 187–227 (1998)
158. Chyzak, F., Mishna, M., Salvy, B.: Effective scalar products for D-finite symmetric functions. J. Comb. Theory A **112**(1), 1–43 (2005)
159. Chyzak, F., Kauers, M., Salvy, B.: A non-holonomic systems approach to special function identities. In: Proceedings of the ISSAC'09, pp. 111–118 (2009)
160. Cluzeau, T., van Hoeij, M.: A modular algorithm to compute the exponential solutions of a linear differential operator. J. Symb. Comput. **38**(3), 1043–1076 (2004)
161. Cluzeau, T., van Hoeij, M.: Computing hypergeometric solutions of linear recurrence equations. Appl. Algebra Eng. Commun. Comput. **17**, 83–115 (2006)
162. Cohn, R.M.: Difference Algebra. Interscience Publishers, John Wiley & Sons, New York (1965)
163. Collins, G.E.: Subresultants and reduced polynomial remainder sequences. J. ACM **14**(1), 128–142 (1967)
164. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms, 2nd edn. Cambridge University Press, Cambridge (2001)
165. Cormier, O., Singer, M.F., Ulmer, F.: Computing the Galois group of a polynomial using linear differential equations. In: Proceedings of the ISSAC'00, pp. 78–85 (2000)
166. Coutinho, S.C.: A Primer of Algebraic D-Modules. Cambridge University Press, Cambridge (1995)
167. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, Berlin (1992)
168. Czichowski, G.: A note on Gröbner bases and integration of rational functions. J. Symb. Comput. **20**(2), 163–167 (1995)
169. Debeerst, R., van Hoeij, M., Koepf, W.: Solving differential equations in terms of Bessel functions. In: Proceedings of the ISSAC'08, pp. 39–46 (2008)
170. Denef, J., Lipshitz, L.: Power series solutions of algebraic differential equations. Math. Ann **267**, 213–238 (1984)
171. Dickson, L.E.: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. Am. J. Math. **35**, 413–422 (1913)
172. Dong, R., Melczer, S., Mezzarobba, M.: Computing error bounds for asymptotic expansions of regular P-recursive sequences. Technical Report 2212.11742, ArXiv, 2022

173. Dreyfus, T., Hardouin, C., Roques, J., Singer, M.F.: On the nature of the generating series of walks in the quarter plane. Invent. Math. **213**(1), 139–204 (2018)
174. Du, L.: Generalized Integral Bases and Applications in Creative Telescoping. Ph.D Thesis, Johannes Kepler University, 2022
175. Du, H., Huang, H., Li, Z.: A q-analogue of the modified Abramov-Petkovšek reduction. In: Advances in Computer Algebra, pp. 105–129. Springer, Berlin (2018)
176. Du, H., Koutschan, C., Thanatipanonda, T., Wong, E.: Determinants for tiling problems yield to the holonomic ansatz. Eur. J. Comb. 103437 (2022)
177. Duan, R., Ran, H., Zhou, R.: Faster matrix multiplication via asymmetric hashing. Technical Report 2210.10173, ArXiv, 2022
178. Dubois, V., Kammerer, J.-G.: Cryptanalysis of cryptosystems based on non-commutative skew polynomials. In: Proceedings of the Public Key Cryptography. LNCS, vol. 6571, pp. 459–472 (2011)
179. Dumas, J.-G., Pernet, C.: Computational linear algebra over finite fields. In: Handbook of Finite Fields, pp. 514–528 (2013)
180. Dwork, B.: On the zeta function of a hypersurface. Publ. Math. de l'IHES **12**, 5–68 (1962)
181. Dwork, B.: On the zeta function of a hypersurface: II. Ann. Math. **80**, 227–299 (1964)
182. Eder, C., Faugère, J.-C.: A survey on signature-based algorithms for computing Gröbner bases. J. Symb. Comput. **80**(3), 719–784 (2017)
183. Egorychev, G.P.: Integral Representation and the Computation of Combinatorial Sums. AMS, Providence (1984)
184. Eisenbud, D.: Commutative Algebra. Springer, Berlin (1995)
185. Fabry, E.: Sur les intégrales des équations différentielles linéaires à coefficients rationnels. Ph.D Thesis, Paris, 1885
186. Farb, B., Dennis, R.K.: Noncommutative Algebra. Springer, Berlin (2012)
187. Fasenmyer, S.M.C.: Some generalized hypergeometric polynomials. Bull. AMS **53**, 806–812 (1947)
188. Fasenmyer, S.M.C.: A note on pure recurrence relations. Am. Math. Mon. **56**, 14–17 (1949)
189. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**(1–3), 61–88 (1999)
190. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the ISSAC'02 (2002)
191. Faugère, J.-C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero dimensional Gröbner bases by change of ordering. J. Symb. Comput. **16**(4), 329–344 (1993)
192. Fayolle, G., Iasogorodski, R., Malyshev, V.: Random Walks in the Quarter-Plane. Springer, Berlin (1999)
193. Feng, R., Gao, X.-S.: Rational general solutions of algebraic ordinary differential equations. In: Proceedings of the ISSAC'04, pp. 155–162 (2004)
194. Feng, R., Gao, X.-S.: A polynomial time algorithm to find rational general solutions of first order autonomous ODEs. J. Symb. Comput. **11**, 1–22 (2005)
195. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. Cambridge University Press, Cambridge (2009)
196. Flajolet, P., Gerhold, S., Salvy, B.: On the non-holonomic character of logarithms, powers, and the nth prime function. Electron. J. Comb. **11**(2), #A2 (2005)
197. Frobenius, F.: Über die Integration der linearen Differentialgleichungen durch Reihen. J. Reine Ange. Math. **76**, 214–235 (1873)
198. Fuchs, L.: Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten. J. Reine Ange. Math. **66**, 121–160 (1866)
199. Furstenberg, H.: Algebraic functions over finite fields. J. Algebra **7**, 271–277 (1967)
200. Galligo, A.: Some algorithmic questions on ideals of differential operators. In: Proceedings of the EUROCAL'85, pp. 413–421 (1985)
201. Garoufalidis, S., Koutschan, C.: The non-commutative A-polynomial of $(-2, 3, n)$ pretzel knots. Exp. Math. **21**(3), 241–251 (2012)

202. Garoufalidis, S., Koutschan, C.: Twisting q-holonomic sequences by complex roots of unity. In: Proceedings of the ISSAC'12, pp. 179–186 (2012)
203. Garoufalidis, S., Koutschan, C.: Irreducibility of q-difference operators and the knot 7_4. Algebraic Geom. Topol. **13**, 3261–3286 (2013)
204. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (1999)
205. Ge, G.: Algorithms related to multiplicative representations of algebraic numbers. Ph.D Thesis, U.C. Berkeley, 1993
206. Geddes, K.O., Czapor, S.R., Labahn, G.: Algorithms for Computer Algebra. Kluwer, Alphen aan den Rijn (1992)
207. Geddes, K.O., Le, H.Q., Li, Z.: Differential rational normal forms and a reduction algorithm for hyperexponential functions. In: Proceedings of the ISSAC'04, pp. 183–190 (2004)
208. Gerhard, J.: Modular Algorithms in Symbolic Summation and Symbolic Integration. LNCS, vol. 3218. Springer, Berlin (2004)
209. Gerhard, J., Giesbrecht, M., Storjohann, A., Zima, E.: Shiftless decomposition and polynomial-time rational summation. In: Proceedings of the ISSAC'03, pp. 119–126 (2003)
210. Gerhold, S.: On some non-holonomic sequences. Electron. J. Comb. **11**(1), 1–8 (2004)
211. Gerhold, S., Glebsky, L., Schneider, C., Weiss, H., Zimmermann, B.: Computing the complexity for Schelling segregation models. Commun. Nonlinear Sci. Numer. Simul. **13**, 2236–2245 (2008)
212. Gessel, I.: Symmetric functions and P-recursiveness. J. Comb. Theory Series A **53**, 257–285 (1990)
213. Giesbrecht, M.: Factoring in skew-polynomial rings. In: Proceedings of the LATIN'92. LNCS, vol. 583, pp. 191–203 (1992)
214. Giesbrecht, M.: Factoring in skew-polynomial rings over finite fields. J. Symb. Comput. **26**(4), 463–486(1998)
215. Giesbrecht, M., Kim, M.S.: Computing the Hermite form of a matrix of Ore polynomials. J. Algebra **376**, 341–362 (2013)
216. Giesbrecht, M., Zhang, Y.: Factoring and decomposing Ore polynomials over $\mathbb{F}_q(t)$. In: Proceedings of the ISSAC'03, pp. 127–134 (2003)
217. Giesbrecht, M., Huang, H., Labahn, G., Zima, E.: Efficient rational creative telescoping. J. Symb. Comput. **109**, 57–87 (2022)
218. Giorgi, P., Jeannerod, C.-P., Villard, G.: On the complexity of polynomial matrix computations. In: Proceedings of the ISSAC'03, pp. 135–142 (2003)
219. Gómez-Torrecillas, J.: Basic module theory over non-commutative rings with computational aspects of operator algebras. In: Algebraic and Algorithmic Aspects of Differential and Integral Operators. LNCS, vol. 8372, pp. 23–82 (2014)
220. Good, I.: Short proof of a conjecture by Dyson. J. Math. Phys. **11**(6), 1884 (1970)
221. Gosper, W.: Decision procedure for indefinite hypergeometric summation. Proc. Natl. Acad. Sci. **75**, 40–42 (1978)
222. Gould, H.: Combinatorial Identities. West Virginia University, Morgantown (1972)
223. Graham, R.L., Knuth, D.E., Patashnik, O.: Concrete Mathematics, 2nd edn. Addison-Wesley, Boston (1994)
224. Griffith, P.A.: On the periods of certain rational integrals: I. Ann. Math. **90**(3), 460–495 (1969)
225. Griffith, P.A.: On the periods of certain rational integrals: II. Ann. Math. **90**(3), 496–541 (1969)
226. Grigoriev, D.Y.: Complexity of factoring and calculating the GCD of linear ordinary differential operators. J. Symb. Comput. **10**(1), 7–37 (1990)
227. Guo, Q.-H., Hou, Q.-H., Sun, L.H.: Proving hypergeometric identities by numerical verifications. J. Symb. Comput. **43**(12), 895–907 (2008)
228. Guo, L., Regensburger, G., Rosenkranz, M.: On integro-differential algebras. J. Pure Appl. Algebra **218**(3), 456–473 (2014)
229. Harris, W.A., Sibuya, Y.: The reciprocals of solutions of linear ordinary differential equations. Adv. Math. **58**(2), 119–132 (1985)

230. Harris, W.A., Sibuya, Y.: The nth roots of solutions of linear ordinary differential equations. Proc. AMS **97**, 207–211 (1986)
231. Harvey, D., van der Hoeven, J.: Integer multiplication in $\mathrm{O}(n \log n)$. Ann. Math. **193**(2), 563–617 (2021)
232. Harvey, D., van der Hoeven, J.: Polynomial multiplication over finite fields in time $\mathrm{O}(n \log n)$. J. ACM **69**(2), 12 (2022)
233. Hebisch, W., Rubey, M.: Extended Rate, more GFUN. J. Symb. Comput. **46**(8), 889–903 (2011)
234. Hendriks, P.A., Singer, M.F.: Solving difference equations in finite terms. J. Symb. Comput. **27**(3), 239–259 (1999)
235. Henrici, P.: Applied and Computational Complex Analysis, vol. 1. John Wiley, New York (1974)
236. Hermite, C.: Sur l'intégration de fractions rationnelles. Ann. Sci. l'É.N.S **2**(1), 215–218 (1872)
237. Hermite, C.: Sur la généralisation des fractions continues algébraiques. Ann. Math. Pura Appl. Sér 2 **21**, 289–308 (1893)
238. Hessinger, S.: Computing Galois Groups of Linear Differential Equations of Order Four. Ph.D Thesis, North Carolina State University, 1997
239. Horn, P., Koepf, W., Sprenger, T.: m-fold hypergeometric solutions of linear recurrence equations revisited. Math. Comput. Sci. **6**(1), 61–77 (2012)
240. Hou, Q.-H., Liu, K.: Congruences and telescopings of P-recursive sequences. J. Differ. Equ. Appl. **27**(5), 686–697 (2021)
241. Hou, Q.-H., Mu, Y.-P.: Minimal universal denominators for linear difference equations. J. Differ. Equ. Appl. **17**(6), 977–986 (2011)
242. Huang, H.: New bounds for hypergeometric creative telescoping. In: Proceedings of the ISSAC'16, pp. 279–286 (2016)
243. Humenberger, A., Jaroschek, M., Kovács, L.: Automated generation of non-linear loop invariants utilizing hypergeometric sequences. In: Proceedings of the ISSAC'17, pp. 221–228 (2017)
244. Hyun, S.G., Melczer, S., St-Pierre, C.: A fast algorithm for solving linearly recurrent sequences. Commun. Comput. Algebra **52**(3), 100–103 (2018)
245. Imamoglu, E., van Hoeij, M.: Computing hypergeometric solutions of second order linear differential equations using quotients of formal solutions and integral bases. J. Symb. Comput. **83**, 254–271 (2017)
246. Immink, G.K., On the relation between linear difference and differential equations with polynomial coefficients. Math. Nach. **200**, 59–76 (1999)
247. Ince, E.L.: Ordinary Differential Equations. Dover, New York (1926)
248. Jaroschek, M.: Improved polynomial remainder sequences for Ore polynomials. J. Symb. Comput. **58**, 64–76 (2013)
249. Jaroschek, M.: Removable Singularities of Ore Operators. Ph.D Thesis, Johannes Kepler University, 2013
250. Johansson, F.: Arb: a C library for ball arithmetic. Commun. Comput. Algebra **47**(4), 166–169 (2013)
251. Johansson, F.: Evaluating parametric holonomic sequences using rectangular splitting. In: Proceedings of the ISSAC'14, pp. 256–263 (2014)
252. Johansson, F.: Fast and rigorous computation of special functions to high precision. Ph.D Thesis, Johannes Kepler Unversity, 2014
253. Johansson, F.: Arb: efficient arbitrary-precision midpoint-radius interval arithmetic. IEEE Trans. Comput. **66**(8), 1281–1292 (2017)
254. Johansson, F., Kauers, M., Mezzarobba, M.: Finding hyperexponential solutions of linear ODEs by numerical evaluation. In: Proceedings of the ISSAC'13, pp. 211–218 (2013)
255. Kaltofen, E., Shoup, V.: Subquadratic-time factoring of polynomials over finite fields. Math. Comput. **67**(223), 1179–1197 (1998)

256. Kandri-Rody, A., Weispfenning, V.: Non-commutative Gröbner bases in algebras of solvable type. J. Symb. Comput. **9**(1), 1–26 (1990)
257. Kaplansky, I.: An Introduction to Differential Algebra, 2nd edn. Hermann (1976)
258. Karr, M.: Summation in finite terms. J. ACM **28**, 305–350 (1981)
259. Karr, M.: Theory of summation in finite terms. J. Symb. Comput. **1**(3), 303–315 (1985)
260. Kashiwara, M.: On the holonomic systems of linear differential equations, II. Invent. Math. **49**, 121–135 (1978)
261. Kauers, M.: Summation algorithms for Stirling number identities. J. Symb. Comput. **42**(11), 948–970 (2007)
262. Kauers, M.: Guessing handbook. Technical Report 09-07, RISC-Linz, 2009
263. Kauers, M.: A Mathematica package for computing asymptotic expansions of solutions of P-finite recurrence equations. Technical Report 11-04, RISC-Linz, 2011
264. Kauers, M.: The holonomic toolkit. In: Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions. Texts and Monographs in Symbolic Computation, pp. 119–144. Springer, Berlin (2013)
265. Kauers, M.: Bounds for D-finite closure properties. In: Proceedings of the ISSAC'14, pp. 288–295 (2014)
266. Kauers, M.: Algorithms for D-finite functions. JNCF'15 Course notes, 2015
267. Kauers, M., Mezzarobba, M.: Multivariate Ore polynomials in SageMath. Commun. Comput. Algebra **53**(2), 57–60 (2019). Software Demonstration at ISSAC'19
268. Kauers, M., Paule, P.: The Concrete Tetrahedron. Springer, Berlin (2011)
269. Kauers, M., Pogudin, G.: Bounds for substituting algebraic functions into D-finite functions. In: Proceedings of the ISSAC'17, pp. 245–252 (2017)
270. Kauers, M., Schneider, C.: Application of unspecified sequences in symbolic summation. In: Proceedings of ISSAC'06, pp. 177–183 (2006)
271. Kauers, M., Schneider, C.: Indefinite summation with unspecified sequences. Discrete Math. **306**(17), 2073–2083 (2006)
272. Kauers, M., Schneider, C.: Partial denominator bounds for partial linear difference equations. In: Proceedings of the ISSAC'10, pp. 211–218 (2010)
273. Kauers, M., Schneider, C.: A refined denominator bounding algorithm for multivariate linear difference equations. In: Proceedings of the ISSAC'11, pp. 201–208 (2011)
274. Kauers, M., Verron, T.: Why you should remove zeros from data before guessing. Commun. Comput. Algebra **53**(3), 126–129 (2019) Poster at ISSAC'19.
275. Kauers, M., Yen, L.: On the length of integers in telescopers for proper hypergeometric terms. J. Symb. Comput. **66**(1–2), 21–33 (2015)
276. Kauers, M., Zeilberger, D.: Factorization of C-finite sequences. In: Proceedings of the WWCA-2016, pp. 131–148 (2018)
277. Kauers, M., Jaroschek, M., Johansson, F.: Ore polynomials in Sage. In: Computer Algebra and Polynomials. LNCS, vol. 8942, pp. 105–125. Springer, Berlin (2014)
278. Kedlaya, K., Umans, C.: Fast polynomial factorization and modular composition. SIAM J. Comput. **40**(6) (2011)
279. Knuth, D.E.: The Art of Computer Programming. Fundamental Algorithms, vol. I. Addison-Wesley, Boston (1968)
280. Knuth, D.E.: The Art of Computer Programming. Seminumerical Algorithms, vol. II. Addison-Wesley, Boston (1969)
281. Knuth, D.E.: The Art of Computer Programming. Sorting and Searching, vol. III. Addison-Wesley, Boston (1973)
282. Koepf, W.: Power series in computer algebra. J. Symb. Comput. **13**, 581–603 (1992)
283. Koepf, W.: Hypergeometric Summation: An Algorithmic Approach to Summation and Special Function Identities. Vieweg, Wiesbaden (1998)
284. Koepf, W.: Hypergeometric Summation. Springer, Berlin (2014)
285. Kogge, P.M., Stone, H.S.: A parallel algorithm for the efficient solution of a general class of recurrence equations. IEEE Trans. Comput. **C-22**(8), 786–793 (1973)

286. Kontsevich, M., Zagier, D.: Periods. In: Mathematics unlimited–2001 and beyond, pp. 771–808 (2001)
287. Koornwinder, T.H.: On Zeilberger's algorithm and its q-analogue. J. Comput. Appl. Math. **48**, 91–111 (1993)
288. Koornwinder, T.H.: Identities of nonterminating series by Zeilberger's algorithm. J. Comput. Appl. Math. **99**, 449–461 (1998)
289. Koutschan, C.: Advanced Applications of the Holonomic Systems Approach. Ph.D Thesis, Johannes Kepler University, 2009
290. Koutschan, C.: A fast approach to creative telescoping. Math. Comput. Sci. **4**(2–3), 259–266 (2010)
291. Koutschan, C.: HolonomicFunctions (User's Guide). Technical Report 10-01, RISC Report Series, University of Linz, Austria, 2010
292. Koutschan, C., Zhang, Y.: Desingularization in the q-Weyl algebra. Adv. Appl. Math. **97**, 80–101 (2018)
293. Koutschan, C., Kauers, M., Zeilberger, D.: Proof of George Andrews' and David Robbins' q-TSPP-conjecture. Proc. Natl. Acad. Sci. **108**(6), 2196–2199 (2011)
294. Kovacic, J.J.: An Eisenstein criterion for noncommutative polynomials. Proc. AMS **34**, 25–29 (1972)
295. Kovacic, J.J.: An algorithm for solving second order linear homogenous differential equations. J. Symb. Comput. **2**, 3–43 (1986)
296. Kovács, L.: Reasoning algebraically about P-solvable loops. In: International Conference on Tools and Algorithms for the Construction and Analysis of Systems, pp. 249–264. Springer (2008)
297. Kovács, L.: A complete invariant generation approach for P-solvable loops. In: International Andrei Ershov Memorical Conference on Perspectives of System Informatics, pp. 242–256. Springer (2009)
298. Krattenthaler, C.: RATE: a Mathematica guessing machine (1997). Available at http://mat.univie.ac.at/~kratt/rate/rate.html
299. Krattenthaler, C.: Advanced determinant calculus. Seminaire Lotharingien Combinatoire **42**(B42q) (1999)
300. Krattenthaler, C.: Advanced determinant calculus: a complement. Linear Algebra Appl. **411**, 68–166 (2005)
301. Kunwar, V.J., van Hoeij, M.: Second order differential equations with hypergeometric solutions of degree three. In: Proceedings of the ISSAC'13, pp. 235–242 (2013)
302. Lairez, P.: Computing periods of rational integrals. Math. Comput. **85**, 1719–1752 (2016)
303. Lam, T.-Y.: A First Course in Noncommutative Rings. Springer, Berlin (2013)
304. Lang, S.: Algebra. Springer, Berlin (2002)
305. Lazard, D.: Gröbner bases, Gaussian elimination, and resolution of systems of equations. In: Proceedings of the EUROCAL'83, pp. 146–156 (1983)
306. Le, H.Q.: A direct algorithm to construct minimal Z-pairs for rational functions. Adv. Appl. Math. **30**(1–2), 137–159 (2003)
307. Leykin, A.: Algorithmic proofs of two theorems of Stafford. J. Symb. Comput. **38**(6), 1535–1550 (2004)
308. Li, Z.: A Subresultant Theory for Linear Differential, Linear Difference, and Ore Polynomials, with Applications. Ph.D Thesis, Johannes Kepler University, 1996
309. Li, Z.: A subresultant theory for Ore polynomials with applications. In: Proceedings of the ISSAC'98, pp. 132–139 (1998)
310. Li, Z.: Lecture notes on decompositions of linear ODE's. Technical Report 19, MM Research Preprints, Beijing, 2000
311. Li, Z.: Lecture Notes on Hyperexponential Solutions of Linear Homogeneous ODE's. MM Research Preprints, Beijing (2000)
312. Liouville, J.: Second mémoire sur la détermination des intégrales dont la valeur est algébrique. J. l'École Polytech. **14**, 149–193 (1833)

313. Lipshitz, L.: The diagonal of a D-finite power series is D-finite. J. Algebra **113**, 373–378 (1988)
314. Lipshitz, L.: D-finite power series. J. Algebra **122**(2), 353–373 (1989)
315. Loewy, A.: Über vollständig reduzible lineare homogene Differentialgleichungen. Math. Ann. **62**, 89–117 (1906)
316. MacConnell, J.C., Robson, J.C.: Noncommutative Noetherian Rings. AMS, Providence (1987)
317. MacMahon, P.A.: Combinatory Analysis. Cambridge University Press, Cambridge (1916)
318. Majewicz, J.E.: WZ-style certification and sister Celine's technique for Abel-type identities. J. Differ. Equ. Appl. **2**, 55–65 (1996)
319. Mallinger, C.: Algorithmic manipulations and transformations of univariate holonomic functions and sequences. Master's Thesis, J. Kepler University, Linz, August 1996
320. El Manssour, R.A., Sattelberger, A.-L., Teguia Tabuguia, B.: D-algebraic functions. Technical Report 2301.02512, ArXiv, 2023
321. Melczer, S.: An Invitation to Analytic Combinatorics. Springer, Berlin (2020)
322. Melczer, S., Mezzarobba, M.: Sequence positivity through numeric analytic continuation: uniqueness of the Canham model for biomembranes. Comb. Theory **2**(2), #4 (2022)
323. Mezzarobba, M.: NumGfun: a package for numerical and analytic computation with D-finite functions. In: Proceedings of the ISSAC'10, pp. 139–146 (2010)
324. Mezzarobba, M.: Autour de l'évaluation numérique des fonctions D-finies. Ph.D Thesis, École polytechnique, 2011
325. Mezzarobba, M.: Rigorous multiple-precision evaluation of D-finite functions in SageMath. Technical Report 1607.01967, ArXiv, 2016
326. Mezzarobba, M.: Truncation bounds for differentially finite series. Ann. Heni Lebesgue **2**, 99–148 (2019)
327. Mezzarobba, M., Salvy, B.: Effective Bounds for P-Recursive Sequences. J. Symb. Comput. **45**(10), 1075–1096 (2010)
328. Mignotte, M.: Mathematics for Computer Algebra. Springer, Berlin (1992)
329. Miller, J.C.P., Brown, D.J.S.: An algorithm for evaluation of remote terms in a linear recurrence sequence. Comput. J. **9**, 188–190 (1966)
330. Mishna, M.: Analytic Combinatorics: A Multidimensional Approach. CRC Press, Boca Raton (2019)
331. Mohammed, M., Zeilberger, D.: Sharp upper bounds for the orders of the recurrences outputted by the Zeilberger and q-Zeilberger algorithms. J. Symb. Comput. **39**(2), 201–207 (2005)
332. Mora, T.: Gröbner bases for non-commutative polynomial rings. In: Proceedings of the AAECC3. LNCS, vol. 229, pp. 353–362 (1986)
333. Mora, T.: An introduction to commutative and noncommutative Gröbner bases. Theor. Comput. Sci. **134**(1), 131–173 (1994)
334. Nakayama, H., Nishiyama, K., Noro, M., Ohara, K., Sei, T., Takayama, N., Takemura, A.: Holonomic gradient descent and its application to the Fisher–Bingham integral. Adv. Appl. Math. **47**, 639–658 (2011)
335. Newton, I.: The method of fluxions and infinite series; with its application to the geometry of curve-lines. Henry Woodfall, 1671/1736
336. Nishioka, K.: An analogy of Harris-Sibuya theorem in difference algebra. Funkcialaj Ekvacioj **54**, 173–176 (2011)
337. NIST: The digital library of mathematical functions. http://dlmf.nist.gov/.
338. Niven, I.: Formal power series. Am. Math. Mon. **76**(8), 871–889 (1969)
339. Nörlund, N.E.: Vorlesungen über Differenzenrechnung. Grundlehren der Mathematischen Wissenschaften, vol. 13. Springer, Berlin (1924)
340. Noy, M.: Graph enumeration. In: Handbook of Enumerative Combinatorics. Taylor and Francis, Milton Park (2015)
341. Oaku, T., Takayama, N.: Algorithms for D-modules—restriction, tensor product, localization, and local cohomology groups. J. Pure Appl. Algebra **156**(2–3), 267–308 (2001)

342. Odlyzko, A.: Asymptotic enumeration methods. Handbook of Combinatorics, vol. II. Elsevier, Amsterdam (1995)
343. Ore, O.: Sur la forme des fonctions hypergéométriques de plusieurs variables. J. Math. Pures Appl. **9**, 311–326 (1930)
344. Ore, O.: Theory of non-commutative polynomials. Ann. Math. **34**, 480–508 (1933)
345. Ostrogradsky, M.: De l'intégration des fractions rationnelles. Bulletin de la classe physico-mathématique de l'Académie Impériale Sci. Saint-Pétersbourg **4**, 145–167 (1845)
346. Ostrogradsky, M.: De l'intégration des fractions rationnelles. Bulletin de la classe physico-mathématique de l'Académie Impériale Sci. Saint-Pétersbourg **4**, 286–300 (1845)
347. Padé, H.: Sur la représentation approchée d'une fonction pour les fractions rationnelles. Ph.D Thesis, Ecole Normal Superieure, 1892
348. Paramonov, S.V.: On rational solutions of linear partial differential or difference equations. Program. Comput. Softw. **39**(2), 57–60 (2013)
349. Paule, P.: Greatest factorial factorization and symbolic summation. J. Symb. Comput. **20**, 235–268 (1995)
350. Paule, P., Riese, A.: A mathematica q-analogue of Zeilberger's algorithm based on an algebraically motivated approach to q-hypergeometric telescoping. In: Ismail, M.E.H., Rahman, M. (eds.) Special Functions, q-Series and Related Topics. Fields Institute Communications, vol. 14, pp. 179–210. AMS, Providence (1997)
351. Paule, P., Schorn, M.: A Mathematica version of Zeilberger's algorithm for proving binomial coefficient identities. J. Symb. Comput. **20**(5–6), 673–698 (1995)
352. Payne, G.: Multivariate Hypergeometric Terms. Ph.D Thesis, Penn State University, 1997
353. Pemantle, R., Wilson, M.C.: Analytic Combinatorics in Several Variables. Cambridge University Press Cambridge (2013)
354. Petkovšek, M.: Hypergeometric solutions of linear recurrences with polynomial coefficients. J. Symb. Comput. **14**(2–3), 243–264 (1992)
355. Petkovšek, M., Salvy, B.: Finding all hypergeometric solutions of linear differential equations. In: Proceedings of the ISSAC'93, pp. 27–33 (1993)
356. Petkovšek, M., Wilf, H., Zeilberger, D.: $A = B$. AK Peters, Natick (1996)
357. Pillwein, V.: Computer Algebra Tools for Special Functions in High Order Finite Element Methods. Ph.D Thesis, Johannes Kepler University, 2008
358. Pivar, M., Finkelstein, M.: Automation, using LISP, of inductive inference on sequences. In: The Programming Language LISP: Its Operations and Applications, pp. 125–136. Information International, Los Angeles (1964)
359. Poincaré, H.: Sur les equations linéaires aux différentielles ordinaires et aux différences finies. J. AMS **7**(3), 203–258 (1885)
360. Praagman, C.: Fundamental solutions for meromorphic linear difference equations in the complex plane, and related problems. J. Reine Ange. Math. **369**, 101–109 (1986)
361. Puiseux, V.A.: Recherches sur les fonctions algébriques. J. Math. Pures Appl. **15**, 365–480 (1850)
362. Puiseux, V.A.: Nouvelles recherches sur les fonctions algébriques. J. Math. Pures Appl. **16**, 228–240 (1851)
363. Raab, C.: Definite Integration in Difference Fields. Ph.D Thesis, Johannes Kepler University, 2012
364. Rainville, E.D.: Special Functions. Macmillan, New York (1960)
365. Regensburger, G., Rosenkranz, M., Middeke, J.: A skew polynomial approach to integro-differential operators. In: Proceedings of the ISSAC'09, pp. 287–294 (2009)
366. Richardson, D.: Some undecidable problems involving elementary functions of a real variable. J. Symb. Logic **33**(4), 514–520 (1968)
367. Richardson, D., Salvy, B., Shackell, J., van der Hoeven, J.: Asymptotic expansions of exp-log functions. In: Proceedings of the ISSAC'96, pp. 309–313 (1996)
368. Rioboo, R.: Quelques aspects du calcul exact avec des numbres réels. Ph.D Thesis, Université de Paris 6 (1991)
369. Risch, R.H.: The problem of integration in finite terms. Trans. AMS **139**, 167–189 (1969)

370. Risch, R.H.: The solution of the problem of integration in finite terms. Bull. AMS **79**, 605–608 (1970)
371. Ritt, J.F.: Differential Algebra. AMS, Colloquium Publications, New York (1950)
372. Robertz, D.: Recent progress in an algebraic analysis approach to linear systems. Multidimens. Syst. Signal Process. **26**, 349–388 (2015)
373. Rosenkranz, M., Regensburger, G.: Integro-differential polynomials and operators. In: Proceedings of the ISSAC'08, pp. 261–268 (2008)
374. Rosenkranz, M., Regensburger, G.: Solving and factoring boundary problems for linear ordinary differential equations in differential algebras. J. Symb. Comput. **43**, 515–544 (2008)
375. Rothstein, M.: A new algorithm for the integation of exponential and logarithmic functions. In: Proceedings of the 1977 Macsyma Users Conference, pp. 263–274 (1977)
376. Ryabenko, A.A.: Formal solutions of linear ordinary differential equations containing m-hypergeometric series. Program. Comput. Softw. **28**(2), 92–101 (2002)
377. Saito, M., Stumfels, B., Takayama, N.: Gröbner Deformations of Hypergeometric Differential Equations. Springer, Berlin (2000)
378. Salvy, B.: Linear differential equations as a data-structure. Found. Comput. Math. **19**(5), 1071–1112 (2019)
379. Salvy, B., Zimmermann, P.: Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM Trans. Math. Softw. **20**(2), 163–177 (1994)
380. Sato, M., Shintani, T. (notes), Muro, M. (translation).: Theory of prehomogeneous vector spaces (algebraic part). Nagoya Math. J. **120**, 1–34 (1990)
381. Schlesinger, L.: Handbuch der Theorie der linearen Differentialgleichungen, vol. 1. Teubner, German (1895)
382. Schlesinger, L.: Handbuch der Theorie der linearen Differentialgleichungen, vol. 2, part 1. Teubner, German (1897)
383. Schlesinger, L.: Handbuch der Theorie der linearen Differentialgleichungen, vol. 2, part 2. Teubner, German (1898)
384. Schneider, C.: Symbolic Summation in Difference Fields. Ph.D Thesis, Johannes Kepler University, 2001
385. Schneider, C.: A collection of denominator bounds to solve parameterized linear difference equations in $\Pi\Sigma$-extensions. In: Proceedings of the SYNASC'04, pp. 269–282 (2004)
386. Schneider, C.: Symbolic summation with single-nested sum extensions. In: Proceedings of the ISSAC'04, pp. 282–289 (2004)
387. Schneider, C.: Degree bounds to find polynomial solutions of parameterized linear difference equations in $\Pi\Sigma$-fields. Appl. Algebra Eng. Commun. Comput. **16**(1), 1–32 (2005)
388. Schneider, C.: Finding telescopers with minimal depth for indefinite nested sum and product expressions. In: Proceedings of the ISSAC'05, pp. 285–292 (2005)
389. Schneider, C.: Product representations in $\Pi\Sigma$-fields. Ann. Comb. **9**(1), 75–99 (2005)
390. Schneider, C.: Apéry's double sum is plain sailing indeed. Electron. J. Comb. **14**(N5) (2007)
391. Schneider, C.: Simplifying sums in $\Pi\Sigma$-extensions. J. Algebra Appl. **6**, 415–441 (2007)
392. Schneider, C.: Symbolic summation assists combinatorics. Sem. Lothar. Combin. B56b (2007)
393. Schneider, C.: A refined difference field theory for symbolic summation. J. Symb. Comput. **43**, 611–644 (2008)
394. Schneider, C.: Simplifying multiple sums in difference fields. In: Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions. Texts and Monographs in Symbolic Computation, pp. 325–360. Springer, Berlin (2013)
395. Schneider, C.: A difference ring theory for symbolic summation. J. Symb. Comput. **72**(1–2), 82–127 (2016)
396. Schneider, C.: Summation theory II: Characterizations of $R\Pi\Sigma^*$-extensions and algorithmic aspects. J. Symb. Comput. **80**(3), 616–664 (2017)
397. Schneider, C., Blümlein, J. (eds.): Computer Algebra in Quantum Field Theory. Texts and Monographs in Symbolic Computation. Springer, Berlin (2013)

398. Schönhage, A., Strassen, V.: Schnelle Multiplikation großer Zahlen. Computing **7**, 281–292 (1971)
399. Schwarz, F.: A factorization algorithm for linear ordinary differential equations. In: Proceedings of the ISSAC'89, pp. 17–25 (1989)
400. Schwarz, F.: Loewy Decomposition of Linear Differential Equations. Springer, Berlin (2012)
401. Sedgewick, R., Wayne, K.: Algorithms, 4th edn. Addison-Wesley, Boston (2011)
402. Serra, R., Arzelier, D., Joldes, M., Lasserre, J.-B., Rondepierre, A., Salvy, B.: Fast and accurate computation of orbital collision probability for short-term encounters. J. Guidance Control Dyn. **39**(5), 1009–1021 (2016)
403. Shackell, J.: Zero-equivalence in function fields defined by algebraic differential equations. Trans. AMS **336**(1), 151–171 (1993)
404. Shackell, J.: Symbolic Asymptotics. Number 12 in Algorithms and Computation in Mathematics. Springer, Berlin (2004)
405. Sills, A., Zeilberger, D.: Disturbing the Dyson conjecture (in a GOOD way). Exp. Math. **15**(2), 187–191 (2006)
406. Singer, M.F.: Algebraic solutions of nth order linear differential equations. Queens Papers Pure Appl. Math. **54**, 379–420 (1980)
407. Singer, M.F.: Solving homogeneous linear differential equations in terms of second order linear differential equations. Am. J. Math. 663–696 (1985)
408. Singer, M.F.: Liouvillian solutions of linear differential equations with liouvillian coefficients. J. Symb. Comput. **11**(3), 251–273 (1991)
409. Singer, M.F.: Testing reducibility of linear differential operators: a group theoretic perspective. Appl. Algebra Eng. Commun. Comput. **7**, 77–104 (1996)
410. Sloane, N.J.A.: The on-line encyclopedia of integer sequences. http://www.oeis.org/
411. Stafford, J.T.: Module structure of Weyl algebras. J. LMS **s2-18**(3), 429–442 (1978)
412. Stanley, R.P.: Differentiably finite power series. Eur. J. Comb. **1**, 175–188 (1980)
413. Stanley, R.P.: Enumerative Combinatorics, vol. 1. Cambridge Studies in Advanced Mathematics, vol. 49, 2nd edn. Cambridge University Press, Cambridge (1997/2012)
414. Storjohann, A.: High-order lifting and integrality certification. J. Symb. Comput. **36**(3–4), 613–648 (2003)
415. Storjohann, A., Villard, G.: Computing the rank and a small nullspace basis of a polynomial matrix. In: Proceedings of the ISSAC'05, pp. 309–316 (2005)
416. Strassen, V.: Gaussian elimination is not optimal. Numer. Math. **13**, 354–356 (1969)
417. Straub, A.: Multivariate Apéry numbers and supercongruences of rational functions. Algebra Number Theory **8**(8), 1985–2006 (2014)
418. Straub, A.: Supercongruences for polynomial analogs of the Apéry numbers. Proc. AMS **147**(3), 1023–1036 (2019)
419. Strehl, V.: Binomial identities–combinatorial and algorithmic aspects. Discrete Math. **136**, 309–346 (1994)
420. Sun, Y., Wang, D., Ma, X., Zhang, Y.: A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras. In: Proceedings of the ISSAC'12, pp. 351–358 (2012)
421. Tabuguia, B.T., Koepf, W.: Symbolic conversion of holonomic functions to hypergeometric type series. Program. Comput. Softw. **48**, 125–146 (2022)
422. Takayama, N.: Gröbner basis and the problem of contiguous relations. Jpn. J. Appl. Math. **6**, 147–160 (1989)
423. Takayama, N.: An algorithm of constructing the integral of a module. In: Proceedings of the ISSAC'90, pp. 206–211 (1990)
424. Takayama, N.: Gröbner basis, integration and transcendental functions. In: Proceedings of the ISSAC'90, pp. 152–156 (1990)
425. Trager, B.: Algebraic factoring and rational function integration. In: Proceedings of the SYMSAC'76, pp. 219–226 (1976)
426. Trager, B.M.: On the Integration of Algebraic Functions. Ph.D Thesis, MIT, 1984
427. Tsai, H.: Algorithms for Algebraic Analysis. Ph.D Thesis, University of California at Berkeley, 2000

428. Tsai, H.: Weyl closure of a linear differential operator. J. Symb. Comput. **29**(4–5), 747–775 (2000)
429. Tsarev, S.P.: An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator. In: Proceedings of the ISSAC'96, pp. 226–231 (1996)
430. Tsarev, S.P.: On some problems in factorization of linear ordinary differential operators. Program. Comput. Softw. **20**(1), 27–29 (1994)
431. van Barel, M., Bultheel, A.: The computation of non-perfect Padé-Hermite approximants. Numer. Algor. **1**, 285–304 (1991)
432. van der Hoeven, J.: Fast evaluation of holonomic functions. Theor. Comput. Sci. **210**(1), 199–216 (1999)
433. van der Hoeven, J.: Fast evaluation of holonomic functions near and in singularities. J. Symb. Comput. **31**(6), 717–743 (2001)
434. van der Hoeven, J.: A new zero-test for formal power series. In: Proceedings of the ISSAC'02 (2002)
435. van der Hoeven, J.: Efficient accelero-summation of holonomic functions. J. Symb. Comput. **42**(4), 389–428 (2007)
436. van der Hoeven, J.: On effective analytic continuation. Math. Comput. Sci. **1**(1), 111–175 (2007)
437. van der Hoeven, J.: Ball arithmetic. Technical Report hal-00432152, Hal ouverte, 2009
438. van der Hoeven, J.: Constructing reductions for creative telescoping. Appl. Algebra Eng. Commun. Comput. **32**, 575–602 (2021)
439. van der Poorten, A.: A proof that Euler missed... — Apéry's proof of the irrationality for $\zeta(3)$. Math. Intell. **1**, 195–203 (1979)
440. van der Put, M., Singer, M.: Galois Theory of Difference Equations. Lecture Notes in Mathematics, vol. 1666. Springer, Berlin (1997)
441. van der Put, M., Singer, M.: Galois Theory of Linear Differential Equations. Springer, Berlin (2003)
442. van Hoeij, M.: Rational solutions of the mixed differential equation and its application to factorization of differential operators. In: Proceedings of the ISSAC'96, pp. 219–225 (1996)
443. van Hoeij, M.: Factorization of differential operators with rational functions coefficients. J. Symb. Comput. **24**, 537–561 (1997)
444. van Hoeij, M.: Rational solutions of linear difference equations. In: Proceedings of the ISSAC'98, pp. 120–123 (1998)
445. van Hoeij, M.: Finite singularities and hypergeometric solutions of linear recurrence equations. J. Pure Appl. Algebra **139**, 109–131 (1999)
446. van Hoeij, M.: Decomposing a 4th order linear differential equation as a symmetric product. Banach Center Publ. **58**, 89–96 (2002)
447. van Hoeij, M.: Factoring polynomials and the knapsack problem. J. Number Theory **95**, 167–189 (2002)
448. van Hoeij, M.: Solving third order linear differential equations in terms of second order equations. In: Proceedings of the ISSAC'07, pp. 355–360, 2007
449. van Hoeij, M., Yuan, Q.: Finding all Bessel type solutions for linear differential equations with rational function coefficients. In: Proceedings of the ISSAC'10, pp. 37–44, 2010
450. Verbaeten, P.: The automatic construction of pure recurrence relations. ACM Sigsam Bull. **8** (1974)
451. Vöge, M., Guttmann, A.J., Jensen, I.: On the number of benzenoid hydrocarbons. J. Chem. Inf. Model. **42**, 456–466 (2002)
452. Wang, X., Pan, V.Y.: Acceleration of Euclidean algorithm and rational number reconstruction. SIAM J. Comput. **32**(2), 548–556 (2003)
453. Wegschaider, K.: Computer generated proofs of binomial multi-sum identities. Master's Thesis, Johannes Kepler University, 1997
454. Weil, A.: Basic number theory. Grundlehren der mathematischen Wissenschaften. Springer, Berlin (1995)

455. Wiart, J., Wong, E.: Walsh functions, scrambled $(0, m, s)$-nets, and negative covariance: Applying symbolic computation to quasi-Monte Carlo integration. Math. Comput. Simul. **182**, 277–295 (2021)
456. Wilf, H.S.: Generating Functionology. AK Peters, Natick (2006)
457. Wilf, H.S., Zeilberger, D.: Rational functions certify combinatorial identities. J. AMS **3**, 147–158 (1990)
458. Wilf, H.S., Zeilberger, D.: An algorithmic proof theory for hypergeometric (ordinary and q) multisum/integral identities. Invent. Math. **108**, 575–633 (1992)
459. Wimp, J., Zeilberger, D.: Resurrecting the asymptotics of linear recurrences. J. Math. Anal. Appl. **111**, 162–176 (1985)
460. Wolf, K.: Effiziente Algorithmen zur Lösung linearer Differentialgleichungssysteme und zur Faktorisierung linerarer Differentialoperatoren über liouvillschen Körpern. Ph.D Thesis, University of Bonn, 1992
461. Wouodjie, M.M.: On the solutions of holonomic third-order linear irreducible differential equations in terms of hypergeometric functions. Ph.D Thesis, Universität Kassel, 2018
462. Xin, G.: The Ring of Malcev-Neumann Series and the Residue Theorem. Ph.D Thesis, Brandeis University, 2004. arXiv:math.CO/0405133
463. Yen, L.: Contributions to the Proof Theory of Hypergeometric Identities. Ph.D Thesis, University of Pennsylvania, 1993
464. Yen, L.: A two-line algorithm for proving terminating hypergeometric identities. J. Math. Anal. Appl. **198**(3), 856–878 (1996)
465. Yu, T., Chen, J.: Uniqueness of Clifford torus with prescribed isoperimetric ratio. Proc. AMS **150**(4), 1749–1765 (2022)
466. Zeilberger, D.: Sister Celine's technique and its generalizations. J. Anal. Appl. **85**, 114–145 (1982)
467. Zeilberger, D.: A fast algorithm for proving terminating hypergeometric identities. Discrete Math. **80**, 207–211 (1990)
468. Zeilberger, D.: A holonomic systems approach to special function identities. J. Comput. Appl. Math. **32**, 321–368 (1990)
469. Zeilberger, D.: The method of creative telescoping. J. Symb. Comput. **11**, 195–204 (1991)
470. Zeilberger, D.: The holonomic ansatz II: Automatic discovery(!) and proof(!!) of holonomic determinant evaluations. Ann. Comb. **11**(2), 241–247 (2007)
471. Zeilberger, D., Bressoud, D.: A proof of Andrews' q-Dyson conjecture. Discrete Math. **54**(2), 201–224 (1985)
472. Zeilberger, D., Zudilin, W.: Automatic discovery of irrationality proofs and irrationality measures. Int. J. Number Theory **17**(3), 815–825 (2021)
473. Zhang, Y.: Contraction of Ore ideals with applications. In: Proceedings of the ISSAC'16, pp. 413–420 (2016)
474. Zhang, Y.: Univariate Contraction and Multivariate Desingularization of Ore Ideals. Ph.D Thesis, Johannes Kepler University, 2017
475. Zhou, Y., van Hoeij, M.: Fast algorithm for factoring difference operators. Commun. Comput. Algebra **53**(3), 150–152 (2019)
476. Zippel, R.: Effective Polynomial Computation. Springer, Berlin (1993)
477. Zürcher, B.: Rationale Normalformen von pseudo-linearen Abbildungen. Master's Thesis, ETH Zürich, 1994

Index

M. Kauers, *D-Finite Functions*, Algorithms and Computation in Mathematics 30,
https://doi.org/10.1007/978-3-031-34652-1

T