# Enumerative and Algebraic Combinatorics

By D. Zeilberger

## 1 Introduction

*Enumeration*, otherwise known as *counting*, is the oldest mathematical subject, while algebraic combinatorics is one of the youngest. Some cynics claim that algebraic combinatorics is not really a new *subject* but just a new *name* given to enumerative combinatorics in order to enhance its (former) poor image, but algebraic combinatorics is in fact the synthesis of two opposing trends: *abstraction of the concrete* and *concretization of the abstract*. The former trend dominated the first half of the twentieth century, starting with Hilbert's "theological" proof of the fundamental theorem of invariants, in which he showed by abstract means that certain invariants existed, but not how to find them. The latter trend is dominating contemporary mathematics, thanks to the omnipresence of The Mighty Computer.

The abstraction trend consists of the *categorization*, *conceptualization*, *structuralization*, and *fancification* (in short, "Bourbakization" (see BOURBAKI)) of mathematics. Enumeration did not escape this trend, and in the hands of such giants as Gian-Carlo Rota and Richard Stanley in America and Marco Schützenberger and Dominique Foata in France, classical, enumerative combinatorics became more conceptual, structural, and algebraic. However, as algebraic combinatorics has established itself as a fully-fledged and separate mathematical speciality, the more recent trend towards the *explicit*, *concrete*, and *constructive* has left its mark as well. It has revealed that many algebraic structures have hidden combinatorial underpinnings; the attempts to unearth these have led to many fascinating discoveries and unsolved problems.

### 1.1 Enumeration

The fundamental theorem of enumeration, independently discovered by several anonymous cave dwellers, states that

$$|A| = \sum_{a \in A} 1.$$

In words: the number of elements in $A$ is the sum over all elements of $A$ of the constant function 1.

While this formula is still useful after all these years, enumerating specific finite sets is no longer considered mathematics. A genuine mathematical fact has to incorporate *infinitely* many facts, and the generic enumeration problem is to enumerate not just one set but all the sets in an infinite family.

To be precise, given an infinite sequence of sets $\{A_n\}_{n=0}^{\infty}$, where each set $A_n$ consists of objects satisfying some combinatorial specifications that depend on the parameter $n$, answer the question, "How many elements does $A_n$ have?"

In a moment we shall look at some examples. But before we can learn how to *answer* this kind of question, let us consider a meta-question: "What is an Answer?"

This was posed, and beautifully answered, by Herbert Wilf. To give some background to Wilf's meta-answer, let us examine answers to some famous instances of enumeration questions.

In the list below, when we are given a set $A_n$ (which will change from example to example), we shall write $a_n$ instead of $|A_n|$. That is, $a_n$ will stand for the number of elements of $A_n$.

**(1) I Ching.** If $A_n$ is the set of all subsets of $\{1, \ldots, n\}$, then $a_n = 2^n$.

**(2) Rabbi Levi Ben Gerson.** If $A_n$ is the set of PERMUTATIONS (see THE SYMMETRIC AND ALTERNATING GROUPS) on $\{1, \ldots, n\}$, then $a_n = n!$.

**(3) Catalan.** If $A_n$ is the set of legal bracketings with $n$ opening brackets and $n$ closing brackets, then $a_n = (2n)!/(n+1)!n!$. (A *legal bracketing* is a sequence of $n$ opening brackets and $n$ closing brackets such that at no point in the sequence has the number of closing brackets exceeded the number of opening brackets. For instance, when $n = 2$ the legal bracketings are [][] and [[]].)

**(4) Leonardo of Pisa.** Let $A_n$ be the set of finite sequences that consist only of 1s and 2s and that sum to $n$. (For example, when $n = 4$ the possible sequences are 1111, 112, 121, 211, and 22.) In this case, we have *three* equivalent answers as follows.

(i)

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$

(ii)

$$a_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k}.$$

(iii) $a_n = F_{n+1}$, where $F_n$ is the sequence *defined* by the recurrence $F_n = F_{n-1} + F_{n-2}$, subject to the initial conditions $F_0 = 0$, $F_1 = 1$.

**(5) Cayley.** If $A_n$ is the set of labeled trees on $n$ vertices, then $a_n = n^{n-2}$. (A *tree* is a connected GRAPH without cycles, and it is *labeled* if the vertices have distinct names.)

**(6)** If $A_n$ is the set of labeled simple graphs with $n$ vertices, then $a_n = 2^{n(n-1)/2}$. (A graph is *simple* if it has neither loops nor multiple edges.)

**(7)** If $A_n$ is the set of labeled *connected* simple graphs on $n$ vertices (that is, graphs for which every vertex can be reached from every other by a path), then $a_n$ is $n!$ times the coefficient of $x^n$ in the power series expansion of

$$\log\left(\sum_{k=0}^{\infty} \frac{2^{k(k-1)/2}}{k!} x^k\right).$$

**(8)** If $A_n$ is the number of LATIN SQUARES of size $n$ ($n \times n$ matrices each of whose rows and columns is a permutation of $\{1, \ldots, n\}$), then $a_n = ???$.

In 1982, Wilf defined an answer as follows.

**Definition.** An *answer* is a *polynomial-time algorithm* (in $n$) for computing $a_n$.

Wilf arrived at this definition after he refereed a paper proposing a "formula" for the answer to question (8), and realized that its "computational complexity" exceeds that of the caveman's formula of direct counting.

What is a "formula"? It is really an algorithm that inputs $n$ and outputs $a_n$. For example, $a_n = 2^n$ is shorthand for the recursive algorithm

*if* $n = 0$ *then* $a_n = 1$,
*else* $a_n = 2 \cdot a_{n-1}$,

which takes $O(n)$ steps. However, using the algorithm

*if* $n = 0$ *then* $a_n = 1$,
*else if* $n$ *is odd, then* $a_n = 2a_{n-1}$,
*else* $a_n = a_{n/2}^2$

takes $O(\log n)$ steps, much faster than Wilf demands. In other cases, like enumerating self-avoiding walks, the best algorithm that is known is exponential, $O(c^n)$, and any lowering of the constant $c$ is a major advance. (A *self-avoiding walk* is a sequence of points $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ in the two-dimensional integer lattice, where each $\boldsymbol{x}_i$ is one of the four neighbours of $\boldsymbol{x}_{i-1}$ and no two of the $\boldsymbol{x}_i$ are equal.) Notwithstanding these exceptions, Wilf's meta-answer is a very useful general guideline for evaluating answers.

The traditional customers of enumeration were mainly probability and statistics. In fact, discrete probability is almost synonymous with enumerative combinatorics, since the probability of an event $E$ occurring is the ratio of the number of successful cases divided by the total number. Also, statistical physics is, by and large, weighted enumeration of lattice models (see PHASE TRANSITIONS AND UNIVERSALITY). About 50 years ago, another important customer came along: computer science. Here one is interested in the *computational complexity* of algorithms: that is, in the number of steps it takes to execute algorithms (see COMPUTATIONAL COMPLEXITY).

## 2 Methods

The following tools are indispensable to the enumerative combinatorialist.

### 2.1 Decomposition

$$|A \cup B| = |A| + |B| \quad (\text{if } A \cap B = \emptyset).$$

In words: the size of the union of two disjoint sets equals the sum of their sizes.

$$|A \times B| = |A| \cdot |B|.$$

In words: the size of the Cartesian product of two sets (that is, the set of all pairs $(a, b)$, where $a \in A$ and $b \in B$) equals the product of their sizes.

$$|A^B| = |A|^{|B|}.$$

In words: the size of the set of functions from $B$ to $A$ equals the size of $A$ raised to the power the size of $B$. For example, the number of 0–1 sequences of length $n$, which can be viewed as functions from $\{1, 2, \ldots, n\}$ to $\{0, 1\}$, equals $2^n$.

### 2.2 Refinement

If

$$A_n = \bigcup_k B_{nk} \quad \text{(disjoint union)},$$

and if $b_{nk}$, the number of elements of $B_{nk}$, is "nice" (and even if it is not), then

$$a_n = \sum_k b_{nk}.$$

The idea here is that it may be possible to take a set $A_n$ that is difficult to count, and split it up into disjoint sets $B_{nk}$ that are easier to count. For example, consider the set $A_n$ of example (4). This can be split into a disjoint union of subsets $B_{nk}$, where each $B_{nk}$ consists of the sequences in $A_n$ that have exactly $k$ 2s. If there are $k$ 2s, then there must be $n - 2k$ 1s, so $b_{nk} = \binom{n-k}{k}$. This yields answer (ii).

### 2.3 Recursion

Suppose that $A_n$ can be decomposed in such a way that it is a combination of fundamental operations applied to the sets $A_{n-1}, A_{n-2}, \ldots, A_0$. Then $a_n$ satisfies a recurrence relation of the form

$$a_n = P(a_{n-1}, a_{n-2}, \ldots, a_0).$$

For example, let $A_n$ be the set of example (4). If a sequence in $A_n$ starts with a 1, then the rest of the sequence must add up to $n - 1$, and if it starts with a 2, then the rest must add up to $n - 2$. Since when $n \geqslant 2$ exactly one of these possibilities occurs and both are possible, we can decompose $A_n$ into $1A_{n-1}$ and $2A_{n-2}$, where $1A_{n-1}$ is shorthand for the set of all sequences that begin with a 1 and continue with a sequence in $A_{n-1}$, and $2A_{n-2}$ is defined similarly. Since the sizes of $1A_{n-1}$ and $2A_{n-2}$ are clearly $a_{n-1}$ and $a_{n-2}$, it follows that $a_n = a_{n-1} + a_{n-2}$, which yields answer (iii).

If $A_n$ is the set of legal bracketings with $n$ pairs (example (3)), then a typical legal bracketing can be written recursively as $[L_1]L_2$, where $L_1$ and $L_2$ are smaller (possibly empty) legal bracketings. For example, if the bracketing is [[][]][[]][[][[]]] then $L_1 = [][]$ and $L_2 = [[]][[][[]]]$. If $L_1$ has $k$ pairs, then $L_2$ has $n - 1 - k$ pairs. It follows that $A_n$ can be identified with the union $\bigcup_{k=0}^{n-1} A_k \times A_{n-1-k}$, and, taking cardinalities, $a_n = \sum_{k=0}^{n-1} a_k a_{n-1-k}$. This is a *nonlinear* (in fact, quadratic) and *nonlocal* recurrence, but it is nevertheless one that satisfies Wilf's dictum.

### 2.4 Generatingfunctionology

According to Wilf, who coined this neologism by making it the title of his classic book (a free download from his website, even though it is still in print!):

> A generating function is a clothesline in which we hang up a sequence of numbers for display.

The method of generating functions is one of the most useful tools of the trade of enumeration. The generating function of a sequence, sometimes called its *z-transform*, is a discrete analog of the LAPLACE transform, and indeed goes back to Laplace himself. If the sequence is $(a_n)_{n=0}^{\infty}$, then its generating function $f(x)$ is defined to be $\sum_{n=0}^{\infty} a_n x^n$. In other words, the terms of the sequence are regarded as the coefficients of a power series in $x$.

Generating functions are so useful because information about the sequence $(a_n)$ translates to information about $f(x)$ that is often easier to process, and after some manipulations one often gets additional information about $f(x)$ that can be translated back into information about the sequence. For example, if $a_0 = a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ when $n \geqslant 2$, then we can do the following manipulations on $f(x)$:

$$\begin{aligned}
f(x) &= \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \sum_{n=2}^{\infty} a_n x^n \\
&= 1 + x + \sum_{n=2}^{\infty} (a_{n-1} + a_{n-2}) x^n \\
&= 1 + x + \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n \\
&= 1 + x + x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} \\
&= 1 + x + x(f(x) - 1) + x^2 f(x) \\
&= 1 + (x + x^2) f(x).
\end{aligned}$$

It follows that

$$f(x) = \frac{1}{1 - x - x^2}.$$

If one performs a partial-fraction decomposition, and expands the two resulting terms in a Taylor series, then one can obtain answer (i) to example (4).

## 3 Weight Enumeration

According to the modern approach, pioneered by Pólya, Tutte, and Schützenberger, generating functions are neither "generating," nor are they functions. Rather, they are *formal power series* that are *weight enumerators* of combinatorial sets. (Usually, but not always, these sets are infinite: for a finite set the corresponding "power series" has only finitely many nonzero terms and is therefore a polynomial.)

A power series $\sum_{n=0}^{\infty} a_n x^n$ is called *formal* when one sheds its analytical connotation as a Taylor series of a function, and thereby obviates the need to worry about convergence. For example, the sum $\sum_{n=0} n!^{n!} x^n$ is perfectly legal as a formal power series even though it converges only when $x = 0$.

As for weight enumerators, consider the following situation. Suppose that we want to study the age distribution of a finite population. One way of doing this is to ask 121 questions. For each $i$ between 0 and 120, we ask those whose age is $i$ to raise their hand. Then we count each of these age-groups one by one, compiling a table of $a_i$ $(0 \leqslant i \leqslant 120)$, and finally computing the generating function

$$f(x) = \sum_{i=0}^{120} a_i x^i.$$

But if the size of the population is much less than 120, it is much more efficient, because fewer questions would be needed, to ask every person their age and then to declare the *weight* of a person of age $i$ to be $x^i$. Then the generating function is the sum of these weights. That is,

$$f(x) = \sum_{\text{persons}} x^{\text{age(person)}},$$

which is a natural extension of the caveman's formula of naive counting. Once we know $f(x)$ we can easily compute statistically interesting quantities, like the *average* and the *variance*, which work out to be $\mu = f'(1)/f(1)$ and $\sigma^2 = f''(1)/f(1) + \mu - \mu^2$, respectively.

The general scenario is that we have an *interesting* (finite or infinite) combinatorial set, let us call it $A$, and a certain numerical *attribute*, $\alpha : A \to \mathbb{N}$, which assigns to each element of $A$ a natural number. (Here we allow 0 as a natural number.) Then the *weight enumerator* of $A$ with respect to $\alpha$ is defined by the formula

$$f(x) = \sum_{a \in A} x^{\alpha(a)}.$$

We shall also use the notation $|A|_x$ for $f(x)$. Obviously, this equals

$$\sum_{n=0}^{\infty} a_n x^n,$$

where $a_n$ is the number of members of $A$ whose $\alpha$ equals $n$. Hence if we have some kind of explicit expression for $f(x)$, we immediately have an "explicit" expression for the actual sequence $a_n$ assuming, that is, that one considers the operations needed to calculate the $n$th coefficient $a_n$ of $f(x)$ as constituting an explicit expression for $a_n$. Even if one does not, then it is still often possible to get a "nice" formula for $a_n$, or, failing this, to extract the asymptotics.

The fundamental operations for naive counting also hold for *weighted counting*: just replace $\|$ by $\|_x$. For example,

$$|A \cup B|_x = |A|_x + |B|_x$$

(if $A \cap B = \emptyset$) and

$$|A \times B|_x = |A|_x \cdot |B|_x.$$

Let us quickly see why the second of these is true. If the members of $A$ and $B$ are endowed with numerical attributes $\alpha$ and $\beta$, respectively, and one defines an attribute $\gamma$ on $A \times B$ by letting $\gamma(a, b)$ equal $\alpha(a) + \beta(b)$, then

$$\begin{aligned} |A \times B|_x &= \sum_{(a,b) \in A \times B} x^{\gamma(a,b)} \\ &= \sum_{(a,b) \in A \times B} x^{\alpha(a) + \beta(b)} \\ &= \sum_{(a,b) \in A \times B} x^{\alpha(a)} \cdot x^{\beta(b)} \end{aligned}$$

$$= \sum_{a\in A}\sum_{b\in B} x^{\alpha(a)}\cdot x^{\beta(b)}$$
$$= \left(\sum_{a\in A} x^{\alpha(a)}\right)\cdot\left(\sum_{b\in B}\cdot x^{\beta(b)}\right)$$
$$= |A|_x\cdot|B|_x.$$

Let us see how these facts can be useful. First, consider the *infinite* set $A$, of all (finite) sequences of 1s and 2s, and let the attribute be "sum of entries." Then the weight of 1221 is $x^6$, and, in general, the weight of a sequence $(a_1\cdots a_r)$ is $x^{a_1+\cdots+a_k}$. The set $A$ can be naturally decomposed as

$$A = \{\phi\}\cup 1A\cup 2A,$$

where $\phi$ is the empty word, and $1A$ is short for the set of all sequences obtained by prefixing a 1 to members of $A$, and analogously for $2A$. Applying $|\cdot|_x$, we get

$$|A|_x = 1 + x|A|_x + x^2|A|_x,$$

which, in this simple case, can be solved *explicitly*, to yield, once again

$$|A|_x = \frac{1}{1-x-x^2}.$$

A legal bracketing $L$ is either empty (in which case the weight is $x^0=1$), or else, as we have already noted, it can be written as $L=[L_1]L_2$, where $L_1$ and $L_2$ are (shorter) legal bracketings. Conversely, whenever $L_1$ and $L_2$ are legal bracketings, so is $[L_1]L_2$. Let $\mathcal{L}$ be the (infinite) set of *all* legal bracketings, and define the weight of a legal bracketing to be $x^n$, where $n$ is the number of bracket pairs [ ]. For example, the weight of [ ] is $x$ and the weight of [ [ ] [ ] [ ] ] is $x^5$. The set $\mathcal{L}$ decomposes naturally as follows:

$$\mathcal{L} = \{\phi\}\cup([\mathcal{L}]\times\mathcal{L}),$$

where $\phi$ denotes the empty word and $[\mathcal{L}]\times\mathcal{L}$ denotes the set of all words of the form $[L_1]L_2$ with $L_1$ and $L_2$ in $\mathcal{L}$. This leads to the *nonlinear* (in fact, quadratic) equation

$$|\mathcal{L}|_x = 1 + x|\mathcal{L}|_x^2,$$

which yields, thanks to the Babylonians, the explicit expression

$$|\mathcal{L}|_x = \frac{1-\sqrt{1-4x}}{2x}.$$

This in turn gives us the answer to example (3) above, via Newton's binomial theorem.

Legal bracketings are equivalent to so-called *binary* trees, that is, unlabelled ordered trees where every vertex has either no children or exactly two children. For instance, when we write the legal bracketing [ [ ] [ ] ] [ [ ] ] [ [ ] [ ] ] ] in the form $[L_1]L_2$ we can think of [ [ ] [ ] ] [ [ ] ] [ [ ] [ ] ] ] as the parent, with children $L_1$ = [ ] [ ] and $L_2$ = [ [ ] ] [ [ ] ] [ [ ] ] ]. Then $L_1$'s children are $\phi$ and [ ], while $L_2$'s are [ ] and [ [ ] [ [ ] ] ]. This process continues until we have reached $\phi$ down every branch of the family.

If we try to count *penta-trees* instead, where each vertex may only have exactly zero or five children, then the generating function, alias weight-enumerator, satisfies the quintic equation

$$f = x + f^5,$$

which, according to ABEL and GALOIS, is not *solvable by radicals* (see THE INSOLUBILITY OF THE QUINTIC). However, solvability by radicals is not everything. Count Joseph LAGRANGE, more than 200 years ago, devised a beautiful and extremely useful formula for extracting the coefficients of the generating function from the equation it satisfies, now called the *Lagrange inversion formula*. Using it one can easily show that the number of complete $k$-ary trees with $(k-1)m+1$ leaves is

$$\frac{(km)!}{((k-1)m+1)!m!}.$$

A multivariate generalization of the Lagrange inversion formula, discovered by the great Bayesian probabilist I. J. Good, enables one to enumerate *colored* trees and many other extensions.

### 3.1 Enumeration Ansatzes

If one wants to turn enumerative combinatorics into a *theory* rather than a collection of solved problems, one needs to introduce *classification*, and *enumeration paradigms* for counting sequences. But since "paradigm" is such a pretentious word, let us use the much humbler German word "ansatz," which roughly means "form of solution."

Let $(a_n)_{n=0}^{\infty}$ be a sequence, and let

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

be its generating function. If we know the "form" of $a_n$, we can often deduce the form of $f(x)$ (and vice versa).

(1) If $a_n$ is a polynomial in $n$, then $f(x)$ has the form
$$f(x) = \frac{P(x)}{(1-x)^{d+1}},$$
where $P$ is a polynomial function and $d$ is the degree of the polynomial that describes $a_n$.

(2) If $a_n$ is a *quasi-polynomial* in $n$ (i.e. there exists an integer $N$ such that for each $r = 0, \dots, N-1$, the function $m \mapsto a_{mN+r}$ is a polynomial in $m$), then, for some (finite) sequence of integers $d_1, d_2, \dots$ and some polynomial function $P$,
$$f(x) = \frac{P(x)}{(1-x)^{d_1}(1-x^2)^{d_2}(1-x^3)^{d_3}\cdots}.$$

(3) If $a_n$ is *C-recursive*, that is, if it satisfies a linear recurrence equation with constant coefficients
$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_d a_{n-d}$$
(a good example is the Fibonacci sequence), then $f(x)$ is a *rational* function of $x$: that is, $f(x) = P(x)/Q(x)$, where $P$ and $Q$ are polynomials.

(4) If $a_n$ satisfies a linear recurrence equation of the form
$$c_0(n)a_n = c_1(n)a_{n-1} + c_2(n)a_{n-2} + \cdots + c_d(n)a_{n-d},$$
where the coefficients $c_i(n)$ are polynomial in $n$, then it is said to be *P-recursive*. (For example, $a_n = n!$ is P-recursive since we have the recurrence $a_n = na_{n-1}$.) If this is the case, then $f(x)$ is *D-finite*, which means that it satisfies a linear differential equation with polynomial coefficients (in $x$).

In the case of $a_n = n!$ the recurrence $a_n = na_{n-1}$ is *first order*. A natural example of a P-recursive sequence satisfying a higher-order linear recurrence with polynomial coefficients is the sequence counting the number of involutions on $\{1, \dots, n\}$. (An involution is a permutation that equals its inverse.) Let us call this number $w_n$. The sequence $(w_n)$ satisfies the recurrence relation
$$w_n = w_{n-1} + (n-1)w_{n-2}.$$
This recurrence follows from the fact that in the permutation $n$ belongs either to a 1-cycle or to a 2-cycle. The former case accounts for $w_{n-1}$ of the involutions, and the latter for $(n-1)w_{n-2}$ of them. (There are $n-1$ ways of choosing the cycle-mate, $i$, say, of $n$, and deleting the resulting cycle leaves an involution of the $n-2$ elements $\{1, \dots, i-1, i+1, \dots, n-1\}$.)

## 4 Bijective Methods

This last argument was a simple example of a *bijective proof*, in this case, of a recurrence for the number of involutions on $n$ objects. Contrast it with the following proof.

The number of involutions of $\{1, \dots, n\}$ with exactly $k$ 2-cycles is
$$\binom{n}{2k}\frac{(2k)!}{k!2^k},$$
because we must first choose the $2k$ elements that will participate in the $k$ 2-cycles, and then match them up into (unordered) pairs, which can be done in $(2k-1)(2k-3)\cdots 1 = (2k)!/(k!2^k)$ ways. Hence
$$w_n = \sum_k \binom{n}{2k}\frac{(2k)!}{k!2^k}.$$
Nowadays such sums can be handled completely *automatically*, and if one inputs this sum to the Maple package EKHAD (downloadable from my website), one would get the recurrence $w_n = w_{n-1} + (n-1)w_{n-2}$ as the output, together with a (completely rigorous!) proof. While the so-called Wilf–Zeilberger (WZ) method can handle many such problems, there are many other cases where one still needs a human proof. In either case such proofs involve (algebraic, and sometimes analytic) *manipulations*. The great combinatorialist Adriano Garsia derogatorily calls such proofs "manipulatorics," and *real enumerators do not manipulate*, or at least try to avoid it whenever possible. The preferred method of proof is by *bijection*.

Suppose one has to prove that $|A_n| = |B_n|$ for every $n$, where $A_n$ and $B_n$ are combinatorial families. The "ugly way" is to get, by some

means or other, algebraic or analytic expressions for $a_n := |A_n|$ and $b_n := |B_n|$. Then one *manipulates* $a_n$ getting another expression $a'_n$, which in turn leads to yet another expression $a''_n$, and if one is patient enough, and clever enough, and in luck, or if the problem is not too deep, one eventually arrives at $b_n$, and the result follows.

On the other hand, the *nice* way of proving that $|A_n| = |B_n|$ is by constructing (a preferably nice) *bijection* $T_n : A_n \to B_n$, which immediately implies, as a corollary, that $|A_n| = |B_n|$ (see Section **??** of THE LANGUAGE AND GRAMMAR OF MATHEMATICS).

In addition to being more *aesthetically* pleasing, a bijective proof is also *philosophically* more satisfactory. In fact the notion of (cardinal) *number* is a highly sophisticated *derived* notion based on the much more basic notion of *being in bijection*. Indeed, according to FREGE, the cardinal numbers are *equivalence classes*, where the equivalence relation is "is in bijective correspondence with" (see Section **??** of THE LANGUAGE AND GRAMMAR OF MATHEMATICS). Saharon Shelah said that people have been exchanging objects, in a one-to-one way, since long before they started to count. Also a bijective proof *explains why* the two sets are equinumerous, as opposed to just certifying the formal correctness of this fact.

For example, suppose that Noah had wanted to prove that there were as many male as female creatures in his Ark. One way of proving this would have been to count the males and count the females, and check that the two resulting numbers were indeed the same. But a much better, conceptual, proof would have been to note that there is an obvious one-to-one correspondence between the set $M$ of males and the set $F$ of females: the function $w : M \to F$ defined by $w(x) = \mathsf{WifeOf}(x)$ is a bijection, with inverse $h : F \to M$ defined by $h(y) = \mathsf{HusbandOf}(y)$.

A classic example of a bijective proof is Glashier's proof of EULER's "odd equals distinct" partition theorem. A *partition* of an integer $n$ is a way of writing it as a sum of positive integers, where order does not matter. For example, 6 has 11 partitions: 6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111. (Here 3111 is shorthand for the sum 3+1+1+1, and so on. Since order does not matter, we count 3111 as the same partition of 6 as 1311, 1131, and 1113. It is convenient to write the partitions with their numbers in decreasing order, as we have done.)

A partition is called *odd* if all its parts are odd, and it is called *distinct* if all its parts are distinct. Let $\mathrm{Odd}(n)$ and $\mathrm{Dis}(n)$ be the sets of odd and distinct partitions of $n$, respectively. For example, $\mathrm{Odd}(6) = \{51, 33, 3111, 111111\}$ and $\mathrm{Dis}(6) = \{6, 51, 42, 321\}$. Euler proved that $|\mathrm{Odd}(n)| = |\mathrm{Dis}(n)|$ for all $n$. His "manipulatorics" proof goes as follows. Let $o(n)$ and $d(n)$ be the number of odd and distinct partitions of $n$, respectively, and let us define the *generating functions* $f(q) = \sum_{n=0}^{\infty} o(n)q^n$ and $g(q) = \sum_{n=0}^{\infty} d(n)q^n$. Using the "multiplication principle" for weighted counting, Euler showed that

$$f(q) = \prod_{i=0}^{\infty} \frac{1}{1-q^{2i+1}}$$

and

$$g(q) = \prod_{i=0}^{\infty} (1+q^i).$$

Using the algebraic identity $1+y = (1-y^2)/(1-y)$, we have

$$\begin{aligned}\prod_{i=0}^{\infty}(1+q^i) &= \prod_{i=0}^{\infty} \frac{1-q^{2i}}{1-q^i} \\ &= \frac{\prod_{i=0}^{\infty}(1-q^{2i})}{\prod_{i=0}^{\infty}(1-q^{2i})\prod_{i=0}^{\infty}(1-q^{2i+1})} \\ &= \prod_{i=0}^{\infty} \frac{1}{1-q^{2i+1}}.\end{aligned}$$

Hence $g(q) = f(q)$, and the identity $o(n) = d(n)$ follows by extracting the coefficient of $q^n$.

For a very long time, these kinds of manipulation were considered to belong to the realm of *analysis*, and in order to justify the manipulations of the infinite series and products, one talked about the "region of convergence," usually $|q| < 1$, and every step had to be justified by the appropriate analytical theorem. Only relatively recently did people come to realize that no analysis need be involved: everything makes sense in the *completely elementary* and much more rigorous (from the philosophical viewpoint) algebra of *formal power series*. One still needs to worry about convergence, so as to exclude, for example, an infinite product like

$\prod_{i=0}^{\infty}(1+x)$, but the notion of convergence in the ring of formal power series is much more user-friendly than its analytical namesake.

Even though invoking analysis was a red herring, Euler's proof, while purely algebraic and elementary, is nevertheless still manipulatorics. It would be much nicer to find a direct bijection between the sets $\mathrm{Dis}(n)$ and $\mathrm{Odd}(n)$. Such a bijection was given by Glaisher. Given a distinct partition, write each of its parts as $2^r \cdot s$, where $s$ is odd, and replace it by $2^r$ copies of $s$. (For example, $12 = 4 \cdot 3$, so we would replace 12 by $3+3+3+3$.) The output is obviously a partition of the same integer $n$, but now into odd parts. For example, the partition $(10, 5, 4)$ is transformed to the new partition $(5, 5, 5, 1, 1, 1, 1)$. To define the inverse transformation, take an odd part $a$ and count how many times it shows up. If it shows up $m$ times, then write $m$ in binary notation, $m = 2^{s_1} + \cdots + 2^{s_k}$, and replace the $m$ copies of $a$ by the $k$ parts: $2^{s_1}a, \ldots, 2^{s_k}a$. It is not hard to check that if you do the first transformation to a partition in $\mathrm{Dis}(n)$ and then do the second transformation, you get back to the partition you started with.

When we perform algebraic (and logical, and even analytical) manipulations, we are really rearranging and combining symbols, and hence we are doing combinatorics in disguise. In fact, *everything is combinatorics*. All we need to do is to take the combinatorics out of the closet, and make it explicit. The plus sign turns into (disjoint) union, the multiplication sign becomes Cartesian product, and induction turns into recursion. But what about the combinatorial counterpart of the minus sign? In 1982, Garsia and Steven Milne filled this gap by producing an ingenious "involution principle" that enables one to translate the implication

$$a = b \quad \text{and} \quad c = d \quad \Rightarrow \quad a - c = b - d$$

into a bijective argument, in the sense that if $C \subset A$ and $D \subset B$, and there are natural bijections $f : A \to B$ and $g : C \to D$ establishing that $|A| = |B|$, and $|C| = |D|$, then it is possible to construct an explicit bijection between $A \backslash C$ and $B \backslash D$. Let us define it in terms of people. Suppose that in a certain village all the adults are married, with the result that there is a natural bijection from the set of married men to the set of married women, $m \mapsto \mathit{WifeOf}(m)$, with its inverse $w \mapsto \mathit{HusbandOf}(w)$. In addition, some of the people have extramarital affairs, but only one per person, and all within the village. There is a natural bijection from the set of cheating men to the set of cheating women, called $m \to \mathit{MistressOf}(m)$, with its inverse $w \to \mathit{LoverOf}(w)$. It follows that there are as many faithful men as there are faithful women. But how do we match them up? (One might imagine, for example, that each faithful man wants a faithful woman to go to church with him.)

Here is how it is done. A faithful man first asks his wife to come with him. If she is faithful, she agrees. If she is not, she has a lover, and that lover has a wife. So she tells her husband: "sorry, hubby, I am going to the pub with my lover, but my lover's wife may be free." If this happens, then the man asks the wife of the lover of his wife to go with him, and if she is faithful, she agrees. If she is not he keeps asking the wife of the lover of the woman who has just rejected his proposal. Since the village is finite, he will eventually get to a faithful woman.

The reaction of the combinatorial enumeration community to the involution principle was mixed. On the one hand it had the universal appeal of a general principle, one that should be useful in many attempts to find bijective proofs of combinatorial identities. On the other hand, its universality is also a major drawback, since involution-principle proofs usually do not give any insight into the *specific* structures involved, and one feels a bit cheated. Such a proof answers the *letter* of the question, but it misses its *spirit*. Given a proof of this kind, one still hopes for a *really* natural, "involution-principle-free proof." This is the case, for instance, with the celebrated Rogers–Ramanujan identity, which states that the number of partitions of an integer into parts that leave remainder 1 or 4 when divided by 5 equals the number of partitions of that integer with the property that the difference between any two parts is at least 2. For example, if $n = 7$ the cardinalities of $\{61, 4111, 1111111\}$ and $\{7, 61, 52\}$ are the same. Garsia and Milne invented their notorious principle in order to give a Rogers–Ramanujan bijection, thereby winning a \$50 prize from George Andrews. However, finding a *really nice* bijective proof is still an open problem.

A quintessential example of a bijective proof is Prüffer's proof of CAYLEY's celebrated result that there are $n^{n-2}$ labeled trees on $n$ vertices

(example (5) earlier). Recall that a labeled tree is a labeled connected simple graph without cycles. Every tree has at least two vertices with only one neighbor (these are called *leaves*). A certain mapping called the *Prüffer bijection* associates with every labeled tree $T$ a vector of integers $(a_1, \ldots, a_{n-2})$, with $1 \leqslant a_i \leqslant n$ for each $i$. This vector is called its *Prüffer code*. Since there are $n^{n-2}$ such vectors, Cayley's formula follows once we have defined the mapping $f$ : Trees $\to$ Codes and proved that it is indeed a bijection. This really needs four steps: defining $f$, defining its alleged inverse map $g$, and proving that $g \circ f$ and $f \circ g$ are the identity maps on their respective domains.

The mapping $f$ is defined recursively as follows. If the tree has 2 vertices, then its code is the empty sequence. Otherwise, let $a_1$ be the (sole) neighbor of the smallest leaf and let $(a_2, \ldots, a_{n-2})$ be the code of the smaller tree obtained by deleting that leaf.

## 5 Exponential Generating Functions

So far, when we have discussed generating functions, we have been talking about *ordinary generating functions* (or OGFs). These are ideally suited for counting ordered structures like integer partitions, ordered trees, and words. But many combinatorial families are really *sets*, where the order is immaterial. For these the natural concept is that of an *exponential generating function* (or EGF).

The EGF of a sequence $\{a(n)\}_{n=0}^{\infty}$ is defined to be

$$\sum_{n=0}^{\infty} \frac{a(n)}{n!} x^n.$$

Labeled objects can be often viewed as sets of smaller *irreducible* objects. For example, a permutation is the disjoint union of *cycles*, a set partition is the disjoint union of *nonempty sets*, a (labeled) forest is the disjoint union of *labeled trees*, and so on.

Suppose that we have two combinatorial families $A$ and $B$, and suppose that there are $a(n)$ labeled objects of size $n$ in the $A$ family, and $b(n)$ in the $B$ family. We can construct a new set of labeled objects $C = A \times B$, where the labels are disjoint and distinct, and define the size of a pair to be the sum of the sizes of the components. We have

$$c(n) = \sum_{k=0}^{n} \binom{n}{k} a(k) b(n-k),$$

since we must

(i) decide the size of the first component, $k$ (an integer between 0 and $n$), which forces the size of the second component to be $n - k$,

(ii) decide which of the $n$ labels go to the first component ($\binom{n}{k}$ ways), and

(iii) pick the objects for each component from the $A$ and $B$ families, respectively, using the available labels ($a(k)b(n-k)$ ways).

Multiplying both sides by $x^n/n!$ and summing from $n = 0$ to $n = \infty$ yields

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{c(n)}{n!} x^n &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{a(k)}{k!} x^k \frac{b(n-k)}{(n-k)!} x^{n-k} \\ &= \left( \sum_{k=0}^{\infty} \frac{a(k)}{k!} x^k \right) \left( \sum_{n-k=0}^{\infty} \frac{b(n-k)}{(n-k)!} x^{n-k} \right).\end{aligned}$$

Hence $\mathrm{EGF}(C) = \mathrm{EGF}(A)\,\mathrm{EGF}(B)$. Iterating, we get

$$\mathrm{EGF}(A_1 \times A_2 \times \cdots \times A_k) = \mathrm{EGF}(A_1) \cdots \mathrm{EGF}(A_k).$$

In particular, if all the $A_i$ are the same, we have that the EGF of ordered $k$-tuples, $A^k$, equals $[\mathrm{EGF}(A)]^k$. But if "order does not matter," then the EGF of $k$-sets of $A$-objects is $[\mathrm{EGF}(A)]^k/k!$, since there are exactly $k!$ ways of arranging a $k$-set into an ordered array (since all labels are distinct, all these objects are different). Summing from $k = 0$ to $k = \infty$ we get the "fundamental theorem of exponential generating functions."

*If $B$ is a labeled combinatorial family that can be viewed as sets of "connected components" that belong to a combinatorial family $A$, then*

$$\mathrm{EGF}(B) = \exp[\mathrm{EGF}(A)].$$

This useful theorem was part of the physics folklore for many years, and was also implicit in many

older combinatorial proofs. However, it was explicated only in the early 1970s. It was fully "categorized" by means of Joyal's theory of species, which grew to be a beautiful theory of enumeration in the hands of the *école Québecoise* (the Labelle and Bergeron *frères*, Leroux, and others).

Here are some venerable examples. Let us try to find the EGF of set partitions. That is, let us try and figure out an expression for

$$\sum_{n=0}^{\infty} \frac{b(n)}{n!} x^n,$$

where $b(n)$ (so-called Bell numbers) denotes the number of set partitions of an $n$-element set.

Recall that a *set partition* of a set $A$ is a set of pairwise-disjoint *nonempty* subsets of $A$, $\{A_1, \ldots, A_r\}$, such that the union of all the $A_i$ equals $A$. For example, the set partitions of the 2-element set $\{1, 2\}$ are $\{\{1\}, \{2\}\}$ and $\{\{1, 2\}\}$.

The atomic objects in this example are *nonempty sets*. (We think of a set $A$ as being the "trivial" partition of itself into just one set.) Let $a(n)$ be the number of ways of partitioning a set of size $n$ into one nonempty set. Clearly when $n = 0$ this cannot be done, so $a(0) = 0$. When $n = 1$ there is exactly one way of doing it, so the EGF of the sequence $a(n)$ is

$$A(x) = 0 + \sum_{n=1}^{\infty} \frac{1}{n!} x^n = \mathrm{e}^x - 1.$$

It follows immediately from the fundamental theorem that

$$\sum_{n=0}^{\infty} \frac{b(n)}{n!} x^n = \mathrm{e}^{\mathrm{e}^x - 1}, \tag{5.1}$$

an identity of Bell. Nowadays, with computer algebra systems, this can be used immediately to crank out the first 100 terms of the sequence $b(n)$. For example, in Maple one simply types

```
taylor(exp(exp(x)-1),x=0,101);
```

so this is definitely an answer in the Wilfian sense. We can also easily derive *recurrences* (albeit ones that need at least $O(n)$ memory), by differentiating both sides of (5.1) and comparing coefficients.

That was really easy, so let us go on and prove something much deeper. How about an EGF-style proof of Levi Ben Gerson's celebrated formula for the number of permutations on $n$ objects, $n!$ (example (2) earlier)? Every permutation can be decomposed into a disjoint union of cycles, so the atomic objects are now *cycles*. How many $n$-cycles are there? The answer is of course $(n-1)!$, since $(a_1, a_2, \ldots, a_n)$ is the same as $(a_2, a_3, \ldots, a_n, a_1)$, which is the same as $(a_3, \ldots, a_n, a_1, a_2)$, etc., which means that we can pick the first entry arbitrarily, after which we have $(n-1)!$ choices for placing the remaining entries. The EGF for cycles is therefore

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{(n-1)!}{n!} x^n &= \sum_{n=1}^{\infty} \frac{1}{n} x^n \\ &= -\log(1-x) = \log(1-x)^{-1}.\end{aligned}$$

Using the fundamental theorem, we get that the EGF of permutations is

$$\begin{aligned}\exp(log(1-x)^{-1}) = (1-x)^{-1} &= \sum_{n=0}^{\infty} x^n \\ &= \sum_{n=0}^{\infty} \frac{n!}{n!} x^n,\end{aligned}$$

and voilà we have a beautiful new proof that the number of permutations on $n$ objects is $n!$.

This argument may not look very impressive. But a slight modification leads immediately to the (ordinary) generating function for the number of permutations on $\{1, \ldots, n\}$ with exactly $k$ cycles, which we shall denote by $c(n, k)$. Here we are fixing $n$ and letting $k$ vary, so the generating function is $C_n(\alpha) = \sum_{k=0}^{n} c(n, k)\alpha^k$. All we have to do to calculate this is go from *naive* counting to *weighted* counting, and assign to each permutation the weight $\alpha^{\#\mathrm{cycles}}$. The fundamental theorem of exponential generating functions carries over word-for-word to weighted counting. The weighted EGF for cycles is $\alpha \log(1-x)^{-1}$, so the weighted EGF for permutations is

$$\exp(\alpha \cdot \log(1-x)^{-1}) = (1-x)^{-\alpha} = \sum_{n=0}^{\infty} \frac{(\alpha)_n}{n!} x^n,$$

where

$$(\alpha)_n := \alpha(\alpha+1)\cdots(\alpha+n-1)$$

is the so-called *rising factorial*. We have therefore derived the far less trivial result that the number of permutations of $\{1, \ldots, n\}$ with exactly $k$ cycles equals the coefficient of $\alpha^k$ in $(\alpha)_n$.

About 10 years ago (Ehrenpreis and Zeilberger 1994) I used this technique to give a combinatorial proof of Pythagoras's theorem in the form

$$\sin^2 z + \cos^2 z = 1.$$

$\sin z$ and $\cos z$ are the weighted EGFs for *increasing sequences* of odd and even lengths, respectively, with weight $(-1)^{[\text{length}/2]}$. Hence the left-hand side is the weighted EGF for ordered pairs of increasing sequences

$$a_1 < \cdots < a_k, \qquad b_1 < \cdots < b_r,$$

such that $k$ and $r$ have the same parity, the sets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_r\}$ are disjoint, and the union of the two sets is $\{1, 2, \ldots, k + r\}$. There is a killer-involution on these sets of pairs defined as follows.

If $a_k < b_r$ then map the pair to

$$a_1 < \cdots < a_k < b_r, \qquad b_1 < \cdots < b_{r-1}.$$

and otherwise map it to

$$a_1 < \cdots < a_{k-1}, \qquad b_1 < \cdots < b_r < a_k.$$

For example, the pair

$$1, 3, 5, 6 \qquad 2, 4, 7, 8, 9, 10, 11, 12,$$

whose sign is $(-1)^2 \cdot (-1)^4 = 1$, goes to the pair

$$1, 3, 5, 6, 12 \qquad 2, 4, 7, 8, 9, 10, 11,$$

whose sign is $(-1)^2 \cdot (-1)^3 = -1$ (and vice versa).

Since this mapping changes the sign, and is an involution, all such pairs can be paired up into mutually cancelling pairs. But this mapping is undefined for one special pair, namely the pair (empty, empty), whose weight is 1, hence the EGF for the sum of the weights of all pairs is 1, explaining the right-hand side.

Yet another application of this method is a proof of André's generating function for the number of *up–down* permutations. A permutation of $a_1 \cdots a_n$ is called up–down (or sometimes *zigzag*) if $a_1 < a_2 > a_3 < a_4 > a_5 < \cdots$. Let $a_n$ be the number of up–down permutations. Then

$$\sum_{n=0}^{\infty} \frac{a(n)}{n!} x^n = \sec x + \tan x.$$

This is equivalent to saying that

$$\cos x \cdot \left( \sum_{n=0}^{\infty} \frac{a(n)}{n!} x^n \right) = 1 + \sin x.$$

Can you find the appropriate set and the killer-involution?

## 6 Pólya–Redfield Enumeration

Often in enumeration it is easy enough to count *labeled* objects, but what about unlabeled ones? For example, the number of labeled (simple) graphs on $n$ vertices (example (6)) is trivially $2^{n(n-1)/2}$, but how many unlabeled graphs are there on $n$ vertices? This is much harder, and in general there are no "nice" answers, but the best known way is via a powerful technique initiated by Pólya, which was largely anticipated by Redfield. Pólya enumeration lends itself very efficiently to counting chemical isomers, since, for example, all the carbon atoms "look the same." Indeed counting isomers was Pólya's initial motivation (see MATHEMATICS AND CHEMISTRY).

The main idea is to view *unlabeled* objects as equivalence classes of easy-to-count *labeled* objects, and to count these equivalence classes. But what is the equivalence? The answer is that there is always a *symmetry group* (see Section **??** of SOME FUNDAMENTAL MATHEMATICAL DEFINITIONS) involved, and it leads to a natural equivalence relation. Let the symmetry group be $G$, and let the set of labeled objects be $A$. Then two objects $a$ and $b$ of $A$ are regarded as *equivalent* if $b = g(a)$ for some member $g$ of the group $G$. This means that there is some symmetry $g$ in the group $G$ that transforms $a$ to $b$. This is easily seen to be an equivalence relation and the equivalence classes are the sets

$$\text{Orbit}(a) := \{g(a) \mid g \in G\}, \quad a \in A,$$

which are known as *orbits*. Calling each orbit a "family," we have the task of counting the number of families. Note that $G$ is a subgroup of the group of permutations of the finite set $A$.

Suppose that there is a picnic consisting of many families and we want to count the number of families. One way would be to define some "canonical head" of each family, say "mother," and count the number of mothers. But some daughters look like

mothers, so this is not so easy. On the other hand, you cannot just count everybody, since then you would count each family several times. The problem is that "naive" counting of people (or objects) is giving a credit of 1 to each person, and this is inappropriate if we are trying to count families. If instead we were to ask each person "How big is your family?" and add to our count the reciprocal of that number, then the calculation would come out just right, since a family of size $k$ would get a credit of $1/k$ for each of its members, and would therefore have been counted exactly once by the end. Going back to counting orbits, we see by the same reasoning that their number is

$$\sum_{a\in A}\frac{1}{|\text{Orbit}(a)|}.$$

The conceptual opposite of "orbit of $a$" is the subgroup of members of $G$ that fix $a$:

$$\text{Fix}(a)=\{g\in G\mid g(a)=a\}.$$

(This is sometimes known as the *stabilizer* of $a$.) To each element $b=ga$ in the orbit of $a$, we can associate the left coset $g\,\text{Fix}(a)$ of $\text{Fix}(a)$. This association turns out to be a well-defined one-to-one correspondence between the orbit of $a$ and the cosets of $\text{Fix}(a)$ in $G$, from which it follows that the size of $\text{Orbit}(a)$ is $|G/\text{Fix}(a)|$. We can therefore substitute $|\text{Fix}(a)|/|G|$ for $1/|\text{Orbit}(a)|$ in the previous formula, which implies that the number of orbits is

$$\frac{1}{|G|}\sum_{a\in A}|\text{Fix}(a)|.$$

Let us use the notation $\chi(\text{statement})$ to stand for 1 if the statement is true and 0 if it is false. Then

$$\begin{aligned}\frac{1}{|G|}\sum_{a\in A}|\text{Fix}(a)| &= \frac{1}{|G|}\sum_{a\in A}\sum_{g\in G}\chi(g(a)=a)\\ &= \frac{1}{|G|}\sum_{g\in G}\sum_{a\in A}\chi(g(a)=a)\\ &= \frac{1}{|G|}\sum_{g\in G}\text{fix}(g),\end{aligned}$$

where $\text{fix}(g)$ is the number of fixed points of $g$ (when $g$ is viewed as a permutation of $A$). We have just proved what used to be called *Burnside's lemma*, but it goes back to CAUCHY and FROBENIUS. It states that the total number of orbits equals the average number of fixed points of $g$, over all transformations $g$ in $G$. If the group $G$ is the full symmetric group of all the permutations of $A$, then the average number of fixed points equals 1 (since in this trivial case there is only one orbit!).

Enter Pólya. The objects that he was interested in counting (e.g. chemical isomers, or colorings of the faces of the cube) were all naturally *functions* from an *underlying set* to a set of *colors* (or atoms). Let us call the underlying set $U$ and the set of colors $C$. A symmetry of $U$ gives rise in a natural way to a transformation of the set of functions $f: U\to C$. Given a function $f$ one defines a new function $gf$ by $g(f)(u):=f(g(u))$. (If we think of $f$ as a coloring, then $gf$ is the new coloring that assigns to $u$ the color that $f$ assigned to $g(u)$.) Now let us think about the number of fixed points of $g$ in the set of $C$-colorings of $U$. Such a fixed point is a coloring $f$ that equals $gf$: that is, $f(u)=f(gu)$ for every $u$. But then $f(u)=f(gu)=f(g^2u)=\cdots$, which means that, given any cycle of $g$, $f$ must assign the same color to all members of that cycle. It follows that the number of fixed colorings of $g$ is $c^{\#\text{cycles}(g)}$, where $c=|C|$ is the number of colors.

Applying Burnside's lemma, we may deduce that the number of different colorings of $U$ (up to $G$-equivalence) is

$$\frac{1}{|G|}\sum_{g\in G}c^{\#\text{cycles}(g)},$$

since an equivalence class of colorings is simply an orbit of one of the colorings in that class.

Here is a simple application. How many necklaces (without a clasp) are there that consist of $p$ beads (where $p$ is a prime) and that use $a$ different colors? The underlying set is $\{0,\dots,p-1\}$, and the symmetry group is $\mathbb{Z}_p$, the cyclic group of order $p$. As usual, regard the elements of the symmetry group as permutations of the set of beads. Since $p$ is a prime, there are $p-1$ elements of $\mathbb{Z}_p$ with one cycle (of length $p$), and one element (the identity permutation) with $p$ cycles (all of length 1). It follows that the number of necklaces is

$$\frac{1}{p}((p-1)\cdot a+1\cdot a^p)=a+\frac{a^p-a}{p}.$$

In particular, since this number is necessarily an integer, we get as a bonus a combinatorial proof of *Fermat's little theorem*: that $a^p-a$ is always a multiple of $p$. Perhaps one day there will be an

equally nice combinatorial proof of Fermat's *last* theorem? All one has to do is to prove that there is no bijection from the union of the set of straight necklaces of size $n$ using $x$ colors, and the set of such necklaces using $y$ colors, to the set of necklaces using $z$ colors (with $n > 2$, of course).

If one wants to keep track of how many beads there are of each color, we simply replace straight counting by weighted counting, and $c^{\#\text{cycles}(g)}$ is replaced by

$$(x_1 + \cdots + x_c)^{\alpha_1} \cdot (x_1^2 + \cdots + x_c^2)^{\alpha_2} \cdots$$

(assuming that $g$ has $\alpha_1$ 1-cycles, $\alpha_2$ 2-cycles, etc.). The resulting expression is the celebrated *cycle-index polynomial*.

### 6.1 The Principle of Inclusion–Exclusion and Möbius Inversion

Another pillar of enumeration is the principle of inclusion–exclusion (nicknamed PIE). Suppose that there are $n$ sins, $s_1, \ldots, s_n$, that a person may succumb to, and suppose that for each set of sins $S$, $A_S$ is the set of people who have all the sins in $S$ (and possibly others). Then the number of good people (without sins) is

$$\sum_S (-1)^{|S|} |A_S|.$$

For example, if the set $A$ is the set of all permutations $\pi$ of $\{1, \ldots, n\}$ and the $i$th sin is having $\pi[i] = i$, then $|A_S| = (n - |S|)!$, and we get that the number of *derangements* (permutations without fixed points) is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!},$$

which yields the *answer*: "closest integer to $n!/\mathrm{e}$." This is sometimes called the "umbrella problem": if on a rainy day $n$ absent-minded people go to a party and leave an umbrella by the door, and if on their departure they each take a random umbrella, then the probability that nobody ends up with the right umbrella is about $1/e$.

The PIE is but a special case of *Möbius inversion* on general partially ordered sets (posets) where the poset happens to be the Boolean lattice. This realization was published in a seminal paper by Rota (1964) and reprinted in his collected works. It is considered by many to be the big bang that started modern algebraic combinatorics. Möbius's original inversion formula is recovered when the partially ordered set is $\mathbb{N}$ and the partial order is divisibility.

A contemporary account of enumeration from the "algebraic" point of view can be found in a marvelous two-volume set by Stanley (2000), which I strongly recommend.

## 7 Algebraic Combinatorics

So far I have described one of the routes to algebraic combinatorics: abstraction and conceptualization of classical enumeration. The other route, "concretization of the abstract," is almost everywhere dense in mathematics, and cannot be described in a few pages. Let me quote from the preface of the excellent *New Perspectives in Algebraic Combinatorics* by Billera et al. (1999).

> Algebraic combinatorics involves the use of techniques from algebra, topology, and geometry in the solution of combinatorial problems, or the use of combinatorial methods to attack problems in these areas. Problems amenable to the methods of algebraic combinatorics arise in these or other areas of mathematics or from diverse parts of applied mathematics. Because of this interplay with many fields of mathematics, algebraic combinatorics is an area in which a wide variety of ideas and methods come together.

### 7.1 Tableaux

An interesting class of objects that initially came up in group representation theory, but that turned out to be useful in many other areas—such as, for example, the theory of algorithms—are *Young tableaux*. They were first used by Reverend Alfred Young to construct *explicit* bases for the irreducible representations of the symmetric group. For any partition $\lambda = \lambda_1 \cdots \lambda_k$ of $n$, a Young tableau of shape $\lambda$ is an array of $k$ left-justified rows with $\lambda_1$ entries in the first row, $\lambda_2$ entries in the second row, and so on, such that every row and every column is increasing, and the set of entries is $\{1, 2, \ldots, n\}$. For example, there are two standard

Young tableaux whose shape is 22,

$$\begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array} \qquad \begin{array}{cc} 1 & 3 \\ 2 & 4 \end{array},$$

and three of shape 31,

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & & \end{array} \qquad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & & \end{array} \qquad \begin{array}{ccc} 1 & 3 & 4 \\ 2 & & \end{array}.$$

Let $f_\lambda$ be the number of standard Young tableaux of shape $\lambda$. For example, for $n = 4$: $f_4 = 1$, $f_{31} = 3$, $f_{22} = 2$, $f_{211} = 3$, and $f_{1111} = 1$. The sum of the squares of these numbers is $1^2+3^2+2^2+3^2+1^2 = 24 = 4!$.

The number $f_\lambda$ is the dimension of the *irreducible representation* parametrized by $\lambda$. It follows by a result in REPRESENTATION THEORY known as *Frobenius reciprocity* that the same is true for all $n$. In other words,

$$\sum_{\lambda \vdash n} f_\lambda^2 = n!,$$

a result known as the *Young–Frobenius identity*. A gorgeous *bijective* proof of this identity, which has many beautiful properties, was given by Gilbert Robinson and Craige Schensted and later extended by Donald Knuth, and is now known as the Robinson–Schensted–Knuth correspondence. It inputs a permutation $\pi = \pi_1\pi_2\cdots\pi_n$, and outputs a pair of Young tableaux of the same shape, thereby proving the identity.

Algebraic combinatorics is currently a very active field, and as mathematics is becoming more and more concrete, constructive and algorithmic, there are going to be many more combinatorial structures discovered in all areas of mathematics (and science!) and this will guarantee that algebraic combinatorialists will stay very busy for a long time to come.

### Further Reading

Billera, L. J., A. Bjorner, C. Greene, R. E. Simion, and R P. Stanley (eds). 1999. *New Perspectives in Algebraic Combinatorics*. Cambridge, UK: Cambridge University Press

Ehrenpreis, L. and D. Zeilbeger. 1994. Two EZ proofs of $\sin^2 z + \cos^2 z = 1$. *American Mathematical Monthly* 101:691.

Rota, G.-C. 1964. On the foundations of combinatorial theory. I. Theory of Möbius functions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete* 2:340–368.

Stanley, R. P. 2000. *Enumerative Combinatorics*, vol. 1. Cambridge, UK: Cambridge University Press.