PCM$_A UPCM001$
document
Enumerative and Algebraic Combinatorics

D. Zeilberger
Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA.

Enumeration, alias *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 20th century, starting with Hilbert's 'theological' proof of the fundamental theorem of invariants, while the latter trend is dominating contemporary mathematics, thanks in large part to Its Omnipresence, The Mighty Computer.

The *abstraction* trend, that consists of *categorization*, *conceptualization*, *structuralization* and *fancification* (in short 'Bourbakisation') of mathematics, did not escape enumeration, 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. On the other hand, the trend towards the *explicit*, *concrete*, and *constructive* revealed that many algebraic structures have hidden combinatorial underpinnings, and the attempts to unearth them lead to the other route towards the establishment of Algebraic Combinatorics as a full-fledged separate mathematical specialty.

Enumeration

The Fundamental Theorem of Enumeration, independently discovered by several anonymous cave-dwellers, states that

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

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:

Given an infinite sequence of sets $\{A(n)\}_{n=0}^{\infty}$, parameterized by n, of objects satisfying a set of **combinatorial specifications**, answer the following

Question: *What is* $a(n) := |A(n)|$?

But before we can learn how to *answer* this kind of questions, let's consider a

Meta-Question: What is an Answer?

It was posed, and beautifully answered by Herbert Wilf. Before telling you Wilf's meta-answer, let's first examine answers to some famous instances of **enumeration questions**.

1. (I Ching) If $A(n)$ is the set of **subsets of** $\{\mathbf{1}, \ldots, \mathbf{n}\}$, then $a(n) = 2^n$.
2. (Levi Ben Greson) If $A(n)$ is the set of **permutations** on $\{1, \ldots, n\}$, then $a(n) = n!$.
3. (Catalan) If $A(n)$ is the set of **complete binary trees** with n leaves, then $a(n) = \frac{(2n-2)!}{(n-1)!n!}$.
4. (Leonardo of Pisa) If $A(n)$ is the set of **words in the alphabet** $\{1, 2\}$ **that sum to** n, then we have *three* answers.

(i)

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

(ii)

$$a(n) = \sum_{k=0}^{n/2} \binom{n-k}{k} \quad .$$

(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 $a(n) = n^{n-2}$.

6. If $A(n)$ is the set of **labeled simple graphs** on n vertices, then $a(n) = 2^{n(n-1)/2}$.

7. If $A(n)$ is the set of **labeled connected simple graphs** on n vertices, then $a(n)$ is $n!$ times the coefficient of x^n in the power series expansion of

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

8. If $A(n)$ is the number of **Latin Squares** of size n ($n \times n$ matrices each of whose rows and column is a permutation of $\{1, \ldots, n\}$), then $a(n) =???$.

In 1982, Herb 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 realizing 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* 1 *else* $2a(n-1)$", that takes $O(n)$ steps. However using the algorithm: "*if* $n = 0$ *then* 1, *else if* n *is odd, then* $2a(n-1)$, *else,* $a(n/2)^2$, takes $O(\log n)$ steps, much faster than Wilf demands. In other cases, like enumerating so-called *Self-Avoiding Walks*, where the best known algorithm is exponential, $O(c^n)$, any lowering of the c is a major advance. 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**. About fifty years ago, another important customer came along: **computer science**, where one is interested in **computational complexity** of **algorithms**, that is in the **number** of steps it takes to execute algorithms.

METHODS

- **Decomposition**:

$$|A \cup B| = |A| + |B| \quad ,$$

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

$$|A \times B| = |A| \cdot |B| \quad ,$$

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

- **Refinement**:

If

$$A(n) = \bigcup_k B(n,k) \quad (disjoint \quad union) \quad ,$$

and if $b(n,k) := |B(n,k)|$ is 'nice' (and even if it isn't), then

$$a(n) = \sum_k b(n,k) \quad .$$

For example, the set $A(n)$ of example **4**, can be split into a disjoint union of the subsets $B(n,k)$, consisting of those sequences with exactly k 2's. Then there must be $n - 2k$ 1's and we have that $b(n,k)$ equals $\binom{n-k}{k}$, yielding answer **(ii)**.

- **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 an 'explicit' recursion

$$a(n) = P(a(n-1), a(n-2), \ldots, a(0)) \quad .$$

For example if $A(n)$ is the set of ex. 4, then for any $n \geq 2$,

$$A(n) \leftrightarrow A(n-1) \times \{1\} \cup A(n-2) \times \{2\} \quad ,$$

yielding answer **(iii)**.

If $A(n)$ is the set of (complete) binary trees on n leaves (ex. 3), then, by considering the number of leaves of the left subtree, we get $A(n) = \bigcup_{k=1}^{n-1} A(k) \times A(n-k)$, and taking cardinalities, $a(n) = \sum_{k=1}^{n-1} a(k) \cdot a(n-k)$, a *non-linear* (quadratic) and *non-local* recurrence, but nevertheless one that satisfies Wilf's dictum.

- **Generatingfunctionology**

According to Herb 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.

$$\{a_n\}_{n=0}^{\infty} \rightarrow f(x) := \sum_{n=0}^{\infty} a_n x^n \quad .$$

Generating functions are so useful because information about a_n translates to information about $f(x)$ that is often easier to process, getting additional information about $f(x)$ that often translates back to information about the sequence. For example, $a_n = a_{n-1} + a_{n-2}$ $(n \geq 2)$ together with the initial conditions $a_0 = 1, a_1 = 1$ translates to

$$f(x) := \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \sum_{n=2}^{\infty} a_n x^n =$$

$$1 + x + \sum_{n=2}^{\infty} (a_{n-1} + a_{n-2}) x^n =$$

$$1 + x + \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n$$

$$1 + x + x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} =$$

$$1 + x + x(f(x) - 1) + x^2 f(x) = 1 + (x + x^2) f(x) \quad .$$

Hence

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

that after performing a partial-fraction decomposition, and taylor-expanding the two resulting terms, would yield ans. **(i)** to ex. 4.

Weight-Enumeration

According to the **modern** approach, pioneered by Pólya, Tutte, and Schützenberger, generating functions are neither 'generating', nor are they functions. They are rather *formal power series* that are *weight enumerators* of (usually infinite) combinatorial sets.

Suppose that we want to study the age distribution of a finite population. One way would be 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, $(0 \leq i \leq 120)$, and finally computing the generating function

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

But if the size of the population is much less than 120, it would be much more efficient to ask every person their age and assign the *weight* of the person to be $x^{age(person)}$.

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

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

The general scenario is that we have an *interesting* (finite of infinite) combinatorial set, let's call it A and a certain numerical *attribute*: $\alpha : A \rightarrow N$. Then the *weight-enumerator* of A w.r.t. to α is defined by

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

Obviously, this equals

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

where a_n is the number of members of A whose α equals n. Hence if we have some kind of explicit expression for $f(x)$, we immediately have an 'explicit' expression for the actual sequence $a_n := Coeff_{x^n} f(x)$, that is, if one allows the operator 'Coeff of x^n' as a primitive (or equivalently, contour integrals in the complex x plane). Even if one doesn't, then it is still often possible to get a 'nice' formula for a_n, and failing this, to extract the **asymptotics**, which is a deep current subspecialty in the hands of such masters as Ed Bender, Rod Canfield, Andrew Odlyzko, and the indefatigable Phillipe Flajolet.

The fundamental operations for naive counting also hold for *weighted counting*, just replace $||$ by $||_x$, to wit:

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

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

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

For example, consider the *infinite* set A, of all words in $\{1, 2\}$, and let the attribute be 'sum of entries', so the weight of 1221. e.g., is x^6, and in general, $weight(a_1 \dots a_r) := x^{a_1 + \dots + a_k}$. The set A can be naturally decomposed as

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

where ϕ is the empty word. Applying $| \cdot |_x$, we get

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

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

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

A *complete* (ordered) binary tree is either the root alone (in which case it only has one vertex), or else the root has two children, called its left-child and right-child, and the subtrees rooted at both of them are complete binary trees on their own right. A *leaf* is a vertex without children. Let B be the (infinite) set of *all* complete binary trees, and define the *weight* of such a tree to be x raised to the power 'the number of leaves'. For example, the weight of () is x and the weight of (()(()())) is x^3. B decomposes naturally into

$$B = \{\cdot\} \cup B \times B \quad ,$$

which leads to the *non-linear* (quadratic) equation

$$|B|_x = x + |B|_x^2 \quad ,$$

that implies, thanks to the Babylonians, the explicit expression

$$|B|_x = \frac{1-\sqrt{1-4x}}{2} \quad ,$$

that in turn, via Newton's binomial theorem, would yield the answer to ex. **3** above.

If instead of complete *binary* trees, where every vertex is allowed either zero or two children, we try to count *penta-trees*, where each vertex may only have exactly zero or five children, then the generating function, alias weight-enumerator, would satisfy the quintic equation

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

that according to Abel and Galois is not *solvable by radicals.* However the *ansatz* of *solvability by radicals* has its limitations. 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 easily gets that the number of complete k-ary trees with $(k-1)m+1$ leaves is:

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

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.

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's use the much humbler German word *ansatz*, that roughly means 'form of solution'.

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

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

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

$$f(x) = \frac{POLY(x)}{(1-x)^{d+1}} \quad ,$$

where d is the degree (in n) of the polynomial describing a_n.

2. If a_n is a *quasi-polynomial* in n (i.e. there exists an integer N such that for each $r = 0, \ldots, N-1$, $a(mN+r)$ is a polynomial in m), then, for some (finitely-many) integers $d_1, d_2, \ldots$,

$$f(x) = \frac{POLY(x)}{(1-x)^{d_1}(1-x^2)^{d_2}(1-x^3)^{d_3}\ldots} \quad .$$

3. If a_n is $C - recursive$, i.e. satisfies a *linear recurrence equation with* **constant** *coefficients* (like the Fibonacci sequence)

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_d a_{n-d} \,,$$

then

$$f(x) = RATIONAL(x) = \frac{POLY(x)}{POLY(x)} \quad .$$

4. If a_n is $P - recursive$, i.e. satisfies a *linear recurrence equation with* **polynomial** *coefficients* (e.g. $a_n = n!$):

$$c_0(n) a_n = c_1(n) a_{n-1} + c_2(n) a_{n-2} + \ldots + c_d(n) a_{n-d} \,,$$

where $c_i(n)$ are polynomials in n, then $f(x)$ is D-finite, i.e. satisfies a *linear differential equation with polynomial coefficients (in x)* .

In the case of $a_n = n!$ the recurrence is *first-order*: $a_n = n a_{n-1}$. 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 $\{1, \ldots, n\}$ (i.e. permutations that equal their inverse), let's call it $\{w_n\}$, that satisfies

$$w_n = w_{n-1} + (n-1) w_{n-2} \quad .$$

This recurrence follows from the fact that n is either in a 1-cycle, or in a 2-cycle, the former case accounting for w_{n-1} of the involutions, and the second for $(n-1)w_{n-2}$ of them ($n-1$ ways of choosing the cycle-mate, i, say, of n, and deleting that cycle leaves an involution of the $n-2$ elements $\{1, \ldots, i-1, i+1, \ldots, n-1\}$.

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 this with the following proof.

The number of involutions of $\{1, \ldots, n\}$ 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 even more 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 *some* (algebraic or analytic) expressions for $a(n) := A(n)$, and $b(n) := |B(n)|$. Then one **manipulates** $a(n)$ getting another expression $a_1(n)$, which in turn leads to yet another expression $a_2(n)$, and if one is patient enough, and clever enough, and in luck, or the problem is not too deep, one would hopefully arrive at $b(n)$, and the result would follow from the transitivity of the equality relation.

On the other hand, the *nice* way of proving that $|A(n)| = |B(n)|$ is by constructing (a preferably nice) *bijection* $T(n) : A(n) \rightarrow B(n)$, which immediately implies, as a corollary, that $|A(n)| = |B(n)|$.

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 'being bijective'. Saharon Shelah said that people have been exchanging objects, in a one-to-one way, 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 wanted to prove that in his Ark, there were as many male as female creatures. One way of proving this was for him to actually have counted the number of males and the number of females, and check that these numbers are indeed the same. But a much better, conceptual, proof is to exhibit the bijection $Males \rightarrow Females$ defined by 'wife of', whose inverse map $Females \rightarrow Males$ is 'husband of'.

A classic example of a bijective proof is Glashier's proof of Euler's Odd=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, hence for convenience's sake it is written as $\lambda_1 \ldots \lambda_k$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k > 0$, summing to n. For example, 6 has 11 partitions: $6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111$.

A partition is called *odd* if all its parts are odd, and it is called *distinct* if all its parts are distinct. Let $Odd(n)$ and $Dis(n)$ be the sets of odd and distinct partitions of n respectively. For example $Odd(6) = \{51, 33, 3111, 111111\}$ and $Dis(6) = \{6, 51, 42, 321\}$. Leonhard Euler proved that $|Odd(n)| = |Dis(n)|$ 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's 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 noted that

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

and

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

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

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

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

$$= \prod_{i=0}^{\infty} \frac{1}{1 - q^{2i+1}} \quad .$$

Hence $g(q) = f(q)$, and $o_n = d_n$ follows by extracting the coefficient of q^n.

For a very long time, these kind of manipulations 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 people came to realize that there is no analysis involved, and every thing 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 set $D(n)$ of distinct partitions and the set $O(n)$ of odd partitions. 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. The output is obviously a partition into odd parts of the same integer n. For example $(10, 5, 4)$ goes to $(5, 5, 5, 1, 1, 1, 1)$. To define the inverse, count for each odd part, a, how many times it shows up, say m times, write m in binary notation: $m = 2^{s_1} + \ldots + 2^{s_k}$, and replace the m copies of a by the k parts : $a \cdot 2^{s_1}, \ldots, a \cdot 2^{s_k}$.

When we perform algebraic (and logical, and even analytical) manipulations, we are really rearranging and *combining* symbols, hence 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, Adriano Garsia and Steven Milne filled this gap by producing an ingenious 'Involution principle' that enables one to translate the implication

$$a = b \quad and \quad c = d \quad \Rightarrow \quad a - c \;=\; b - d \quad ,$$

into a bijective argument, in the sense that if $C \subset A$ and $D \subset B$, and there are natural bijections $f : A \rightarrow B$ and $g : C \rightarrow D$ establishing that $a := |A|$ equals $b := |B|$, and $c := |C|$ equals $d := |D|$, then it is possible to construct an explict bijection between $A \backslash C$ and $B \backslash D$. Let's define it in terms of people. Suppose that in a certain village all the adults are married, and hence there is a natural bijection between the set of married men to the set of married women, $m \rightarrow WifeOf(m)$, with its inverse $w \rightarrow HusbandOf(w)$. In addition, some of the people have extra-marital affairs, (but only one per person, and all within the village). There is a natural bijection between the set of cheating men to the set of cheating women, called $m \rightarrow MistressOf(m)$, with its inverse $w \rightarrow LoverOf(w)$. It follows that there are as many faithful men as there are faithful women. How to match them up? (say if a faithful man wants a faithful woman to go to Church with him). 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, but I am going to the pub with my lover, but my lover's wife may be free, so the man asks the wife of the lover of his wife to go with him, and if she is faithful, she agrees. Is she is not he keeps asking the wife of the lover of the woman who just rejected his proposal, and 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*, 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 misses its *spirit*. In these cases one still hopes for a *really* natural, 'Involution Principle- free proof'. This is the case with the celebrated Rogers-Ramanujan identity that 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 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 (ex. 5 above). 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*). The Prüffer bijection associates with every labeled tree T a vector of integers $(a_1, \ldots, a_{n-2})$, with $1 \leq a_i \leq n$. Since there are n^{n-2} such vectors, Cayley's formula would follow once we define a mapping $f : Trees \rightarrow Codes$ and prove that it is indeed a bijection. This really entails 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.

An even nicer bijective proof was given in 1980 by André Joyal, whose proof formed the *iconic example* of a gorgeous and deep combinatorial theory of *species*.

Many more bijections can be found in Dennis Stanton and Dennis White's lively 'Constructive Combinatorics' (Springer). Bijective combinatorics has reached new summits in the hands of the members of the *ecole bordelaise*, uner the guruship of the great Bijectionist Xavier Viennot and his talented disciples: Mireille Bousquet-Mélou, Maylis Delest, and many others.

Exponential Generating Functions

We already talked above about *ordinary generating functions* (ogf) that 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 *exponential generating function* (egf).

The egf of a sequence $\{a(n)\}_{n=0}^{\infty}$ is

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

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 *non-empty sets*, a (labeled) forest is the disjoint union of *labeled trees*, etc.

Suppose that we have two combinatorial families A and B, and 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

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

since we must decide (i) the size of the first component, k ($k = 0 \dots n$), which forces the size of the second component to be $n-k$. (ii) which of the n labels go to the first component ($\binom{n}{k}$ ways). (iii) pick the objects for each component from the A and B family 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

$$\sum_{n=0}^{\infty} \frac{c(n)}{n!} x^n = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{a(k)}{k!} x^k \frac{b(n-k)}{(n-k)!} x^{n-k} =$$

$$\left(\sum_{k=0}^{\infty} \frac{a(k)}{k!} x^k \right) \left(\sum_{n-k=0}^{\infty} \frac{b(n-k)}{(n-k)!} x^{n-k} \right) \quad .$$

Hence $egf(C) = egf(A) egf(B)$. Iterating, we get

$$egf(A_1 \times A_2 \times \ldots \times A_k) = egf(A_1) \cdots egf(A_k) \quad .$$

In particular, if all the A_i's are the same, we have that the egf of ordered k-tuples, A^k, equals $[egf(A)]^k$. But if 'order does not matter' then the efg of k-sets of A-objects is $[egf(A)]^k/k!$, 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

$$egf(B) = exp[\ egf(A)\ ] \quad .$$

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 1970-ies. It was fully 'categorized' by means of Joyal's theory of species, that grew to be a beautiful theory of enumeration in the hands of the *ecole québecoise* (the Labelle and Bergeron *frères*, Leroux, and others).

Here are some venerable examples. Let's try to find the egf of set partitions, i.e. let's try and figure out an expression for

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

where $b(n)$, (the so-called Bell numbers) denote 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 *non-empty* subsets of A, $\{A_1, \ldots, A_r\}$ such that the union of all the A_i's equals A. For example, the set partitions of the 2-element set $\{1, 2\}$ are $\{\{1\}, \{2\}\}$ and $\{\{1, 2\}\}$.

The *atomic objects* are *non-empty sets*. Let $a(n)$ be the number of non-empty sets of the form $\{1, 2, \ldots, n\}$. Clearly when $n = 0$ there is no such (non-empty) set, and when $n = 1$ there is exactly one such set, so the egf is

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

and we get immediately that

$$\sum_{n=0}^{\infty} \frac{b(n)}{n!} x^n = e^{e^x - 1} \quad . \qquad (Bell)$$

Nowadays, with computer algebra systems, this can be used immediately to crank out the first hundred terms of the sequence $b(n)$ by simply typing, e.g. in Maple:
`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 needing at least $O(n)$ memory), by differentiating both sides of ($Bell$) and comparing coefficients.

That was really easy, so let's go on and prove something much deeper. How about an egf-style proof of Rabbi Levi Ben Gerson's celebrated formula for the number of permutations on n objects, $n!$? (ex. 2 above). Every permutation can be decomposed into a disjoint union of cycles, hence the atomic objects are *cycles.* How many n-cycles are there? $(n-1)!$ of course, 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., so we can pick the first entry arbitrarily, and then we have $(n-1)!$ choices for placing remaining entries. Hence the egf for cycles is:

$$\sum_{n=1}^{\infty} \frac{(n-1)!}{n!} x^n = \sum_{n=1}^{\infty} \frac{1}{n} x^n$$

$$= -\log(1-x) = \log(1-x)^{-1} \quad .$$

Using the Fundamental Theorem of Exponential Generating Functions, we get that the egf of permutations is

$$exp(log(1-x)^{-1}) = (1-x)^{-1} = \sum_{n=0}^{\infty} x^n$$

$$= \sum_{n=0}^{\infty} \frac{n!}{n!} x^n \quad ,$$

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

Isn't it a bit of an over-kill? Perhaps. But a slight modification leads immediately to the (ordinary) generating function for the number of permutations on $\{1, \ldots, n\}$ with exactly k cycles (let's call it $c(n,k)$), with n fixed, $C_n(\alpha) = \sum_{k=0}^{n} c(n,k)\alpha^k$. All we have to do is go from *naive* counting to *weighted* counting, and assign to each permutation the weight $\alpha^{\#cycles}$. The Fundamental Theorem of Exponential Generating Functions goes verbatim to weighted counting. The weighted egf for cycles is $\alpha \log(1-x)^{-1}$, and hence the weighted egf for permutations is

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

where

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

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

About ten years ago (American Mathematical onthly **101** (1994), p. 691)), I used this technique to give a combinatorial proof of the Pythagorean theorem in the form

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

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

$$a_1 < \ldots < a_k \quad ; \quad b_1 < \ldots < b_r \quad ,$$

such that k and r have the same parity , $\{a_1, \ldots, a_k\}$ is disjoint from $\{b_1, \ldots, b_r\}$, and their union 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 it to

$$a_1 < \ldots < a_k < b_r \quad ; \quad b_1 < \ldots < b_{r-1} \quad .$$

and otherwise, map it to:

$$a_1 < \ldots < a_{k-1} \quad ; \quad b_1 < \ldots < b_r < a_k \quad .$$

For example

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

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

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

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 to proving André's generating function for the number of *up-down* permutations. A permutation of $a_1 \ldots a_n$ is up-down (sometimes called *zigzag*) if $a_1 < a_2 > a_3 < a_4 > a_5 < \ldots$. Let $a(n)$ be the number of up-down permutations then

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

This is equivalent to

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

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

Polyá-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 (ex. 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 George Polyá, that was largely anticipated by J.H. Redfield. Polyá enumeration lends itself very efficiently to counting chemical isomers, since, for example, all the Carbon atoms 'look the same'. Indeed counting isomers was Polyá's initial motivation.

The main idea it to view *unlabeled* objects as *equivalence classes* of easy-to-count *labeled objects*, and count these equivalence classes. But 'what equivalence'? There is always a (sometimes hidden) *symmetry group*, let's call it G, 'acting' on the set of labeled objects, let's call it A, by a group action $G \times A \rightarrow A$, $(g,a) \rightarrow g(a)$, and two objects a and b of A are equivalent if $b = g(a)$ for some member g of the group G. This is obviously an equivalence relation and the equivalence classes are the orbits

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

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 on the finite set A.

Suppose that there is picnic consisting of many families, and we want to count the number of families. One way would be to define some 'canonical head' of a family, say 'mother' and count the number of mothers. But some daughters look like mothers, so it is not so easy. On the other hand, you can't just literally count people, since then you would get a gross overcount. But 'naive' counting of people (or objects) is giving a credit of 1 to each person. If we asked each person: 'How big is your family', and add to our count the reciprocal of that number, then things would come out just right, since a family of size k would get credit $1/k$ for each of its members, hence would be counted exactly once. Going back to counting orbits, we see that their number is

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

The conceptual opposite of 'orbit of a' is the subgroup of members of G that fix a,

$$Fix(a) = \{g \in G \,|\, g(a) = a\} \quad .$$

There is a natural one-to-one correspondence between the cosets of $Fix(a)$ in G and the orbit of a, hence the size of $Orbit(a)$ is $|G/Fix(a)|$, and we get (Let $\chi(statement)$ be 1 or 0 according to whether it is true or false, respectively).

$$\#Orbits = \frac{1}{|G|} \sum_{a \in A} |Fix(a)| =$$

$$\frac{1}{|G|} \sum_{a \in A} \sum_{g \in G} \chi(g(a) = a)$$

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{a \in A} \chi(g(a) = a) = \frac{1}{|G|} \sum_{g \in G} fix(g) \quad ,$$

where $fix(g)$ is the number of fixed points of g (viewed as a permutation of A). We have just proved what used to be called *Burnside's lemma* but goes back to Cauchy and Frobenius, that states that the number of orbits in the action of G on A equals the average number of fixed points over G. If the group G is the full symmetric group of all the permutations of A, we get that the average number of fixed points equals 1 (in this trivial case there is only one orbit!).

Enter George Polyà. 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*, let's call it U to a set of *colors* (or atoms), let's call it C. The group of symmetry of U naturally acts on the set of functions $f : U \rightarrow C$ by the *induced action*: $g(f)(u) := f(g(u))$. To find the number of fixed points of g in the set of C-colorings of U simply decompose g into cycles. Such a coloring must have the same color on the members of each cycle, hence if there are $c := |C|$ colors, the number of different colorings of U (up to G-equivalence) is

$$\frac{1}{|G|}\sum_{g \in G} c^{\#Cycles(g)} \quad .$$

Here is a simple application. How many necklaces (without a clasp) are there consisting of p beads (p prime), using a different colors? The underlying set is $\{0, \dots, p-1\}$, and the symmetry group is Z_p, the cyclic group of order p. Since p is a prime, there are $p-1$ elements 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

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

In particular, since this number is necessarily an integer, we get as a bonus a combinatorial proof of *Fermat's Little Theorem*. Who knows? Perhaps one day there would be an equally nice combinatorial proof of Fermat's *Last* theorem? All one has to do is to prove that there is no bijection between the union of the sets of straight necklaces of size n using x colors, and that set using y colors, with that set 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 $c^{\#Cycles(g)}$ is replaced by (assuming that g has α_1 1-cycles, α_2 2-cycles, etc.)

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

The resulting expression is the celebrated *cycle-index polynomial*.

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, $s_1, \dots, s_n$ 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

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

For example, if the set A is the set of all permutations π of $\{1, \dots, n\}$ 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

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

that yields the *answer*: 'closest integer to $n!/e$'.

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*, made in 1964, by Gian-Carlo Rota, in his seminal paper 'On the Foundations of Combinatorial Theory I. Theory of Möbius functions', (reprinted in Rota's Collected Works) is considered by many to be the *big bang* that started modern algebraic combinatorics. Möbius's original inversion formula is gotten back when the partially ordered set is N and the partial order is divisibility.

A contemporary account of Enumeration from the 'algebraic' point of view can be found in Richard Stanley's marvelous two-volume set 'Enumerative Combinatorics' (Cambridge Univ. Press), that I strongly recommend.

Algebraic Combinatorics

So far I described one of the routes to Algebraic Combinatorics: abstraction and conceptualization of classical enumeration. The other route, 'concretization of the abstract' is almost every-where dense in mathematics, and cannot be described in a few pages. Let me quote from the preface of the excellent volume

‘New Perspectives in Algebraic Combinatorics’ by Billera, Björner, Greene, Simion, and Stanley (Cambridge University Press).

“*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.*”

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, for example, the theory of algorithms, are *Young Tableaux.* They were first used by Rev. Alfred Young to construct *explicit* bases for the irreducible representations of the symmetric group. For any partition $\lambda = \lambda_1 \dots \lambda_k$ of n, a Young tableau of shape λ is an array of k left-justified rows with λ_1 entries in the first row, λ_2 entries in the second row, and so on, such that every row and every column is increasing, and the set of entries is $\{1, 2, \dots, n\}$. For example there are two Standard Young Tableaux whose shape is 22:

$$matrix12$$

Since f_λ is the dimension of the irreducible representation parametrized by λ, it follows by so-called *Frobenius reciprocity* that the above is true for all n, in other words:

$$\sum_{\lambda \vdash n} f_\lambda^2 = n! \quad . \qquad (Y-F)$$

A gorgeous *bijective* proof of this identity, that has many beautiful properties, was given by Gilbert Robinson and Craige Schenstead and later extended by Donald Knuth, and is now known as the Robinson-Schenstead-Knuth Correspondence. It inputs a permutation $\pi = \pi_1\pi_2 \dots \pi_n$, and outputs a pair of Young Tableaux of the same shape, thereby proving $(Y-F)$.

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.

*Biography of contributor

Doron Zeilberger was born, as a person, on July 2, 1950. He was born, as a mathematician, in 1976, when he got his Ph.D. under the direction of Harry Dym (in analysis). He was born-again, as a combinatorialist, two years later, when he read a lovely proof of the so-called Hook-Length Formula (enumerating Standard Young Tableaux) by Curtis Greene, Albert Nijenhuis, and Herb Wilf. He lived happily ever after.