Chapter 1

What is Enumerative Combinatorics?

1.1 How to Count

The basic problem of enumerative combinatorics is that of counting the number of elements of a finite set. Usually we are given an infinite collection of finite sets S_i where i ranges over some index set I (such as the nonnegative integers $\mathbb{N}$), and we wish to count the number $f(i)$ of elements in each S_i "simultaneously." Immediate philosophical difficulties arise. What does it mean to "count" the number of elements of S_i? There is no definitive answer to this question. Only through experience does one develop an idea of what is meant by a "determination" of a counting function $f(i)$. The counting function $f(i)$ can be given in several standard ways:

1. The most satisfactory form of $f(i)$ is a completely explicit closed formula involving only well-known functions, and free from summation symbols. Only in rare cases will such a formula exist. As formulas for $f(i)$ become more complicated, our willingness to accept them as "determinations" of $f(i)$ decreases. Consider the following examples.

1.1.1 Example. For each $n \in \mathbb{N}$, let $f(n)$ be the number of subsets of the set $[n] = \{1, 2, \ldots, n\}$. Then $f(n) = 2^n$, and no one will quarrel about this being a satisfactory formula for $f(n)$.

1.1.2 Example. Suppose n men give their n hats to a hat-check person. Let $f(n)$ be the number of ways that the hats can be given back to the men, each man receiving one hat, so that no man receives his own hat. For instance, $f(1) = 0$, $f(2) = 1$, $f(3) = 2$. We will see in Chapter 2 (Example 2.2.1) that

$$f(n) = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \tag{1.1}$$

This formula for $f(n)$ is not as elegant as the formula in Example 1.1.1, but for lack of a simpler answer we are willing to accept (1.1) as a satisfactory formula. It certainly has

the virtue of making it easy (in a sense that can be made precise) to compute the values $f(n)$. Moreover, once the derivation of (1.1) is understood (using the Principle of Inclusion-Exclusion), every term of (1.1) has an easily understood combinatorial meaning. This enables us to "understand" (1.1) intuitively, so our willingness to accept it is enhanced. We also remark that it follows easily from (1.1) that $f(n)$ is the nearest integer to $n!/e$. This is certainly a simple explicit formula, but it has the disadvantage of being "non-combinatorial"; that is, dividing by e and rounding off to the nearest integer has no direct combinatorial significance.

1.1.3 Example. Let $f(n)$ be the number of $n \times n$ matrices $\boldsymbol{M}$ of 0's and 1's such that every row and column of $\boldsymbol{M}$ has three 1's. For example, $f(0) = 1$, $f(1) = f(2) = 0$, $f(3) = 1$. The most explicit formula known at present for $f(n)$ is

$$f(n) = 6^{-n} n!^2 \sum \frac{(-1)^\beta (\beta + 3\gamma)!\, 2^\alpha\, 3^\beta}{\alpha!\, \beta!\, \gamma!^2\, 6^\gamma}, \tag{1.2}$$

where the sum ranges over all $(n+2)(n+1)/2$ solutions to $\alpha + \beta + \gamma = n$ in nonnegative integers. This formula gives very little insight into the behavior of $f(n)$, but it does allow one to compute $f(n)$ much faster than if only the combinatorial definition of $f(n)$ were used. Hence with some reluctance we accept (1.2) as a "determination" of $f(n)$. Of course if someone were later to prove that $f(n) = (n-1)(n-2)/2$ (rather unlikely), then our enthusiasm for (1.2) would be considerably diminished.

1.1.4 Example. There are actually formulas in the literature ("nameless here for evermore") for certain counting functions $f(n)$ whose evaluation requires listing all (or almost all) of the $f(n)$ objects being counted! Such a "formula" is completely worthless.

2. A recurrence for $f(i)$ may be given in terms of previously calculated $f(j)$'s, thereby giving a simple procedure for calculating $f(i)$ for any desired $i \in I$. For instance, let $f(n)$ be the number of subsets of $[n]$ that do not contain two consecutive integers. For example, for $n = 4$ we have the subsets $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,3\}$, $\{1,4\}$, $\{2,4\}$, so $f(4) = 8$. It is easily seen that $f(n) = f(n-1) + f(n-2)$ for $n \geq 2$. This makes it trivial, for example, to compute $f(20) = 17711$. On the other hand, it can be shown (see Section 4.1 for the underlying theory) that

$$f(n) = \frac{1}{\sqrt{5}} \left(\tau^{n+2} - \bar{\tau}^{n+2} \right),$$

where $\tau = \frac{1}{2}(1 + \sqrt{5})$, $\bar{\tau} = \frac{1}{2}(1 - \sqrt{5})$. This is an explicit answer, but because it involves irrational numbers it is a matter of opinion (which may depend on the context) whether it is a better answer than the recurrence $f(n) = f(n-1) + f(n-2)$.

3. An algorithm may be given for computing $f(i)$. This method of determining f subsumes the previous two, as well as method **5** below. Any counting function likely to arise in practice can be computed from an algorithm, so the acceptability of this method will depend on the

elegance and performance of the algorithm. In general, we would like the time that it takes the algorithm to compute $f(i)$ to be "substantially less" than $f(i)$ itself. Otherwise we are accomplishing little more than a brute force listing of the objects counted by $f(i)$. It would take us too far afield to discuss the profound contributions that computer science has made to the problem of analyzing, constructing, and evaluating algorithms. We will be concerned almost exclusively with enumerative problems that admit solutions that are more concrete than an algorithm.

4. An estimate may be given for $f(i)$. If $I = \mathbb{N}$, this estimate frequently takes the form of an *asymptotic formula* $f(n) \sim g(n)$, where $g(n)$ is a "familiar function." The notation $f(n) \sim g(n)$ means that $\lim_{n\to\infty} f(n)/g(n) = 1$. For instance, let $f(n)$ be the function of Example 1.1.3. It can be shown that

$$f(n) \sim e^{-2}36^{-n}(3n)!.$$

For many purposes this estimate is superior to the "explicit" formula (1.2).

5. The most useful but most difficult to understand method for evaluating $f(i)$ is to give its *generating function*. We will not develop in this chapter a rigorous abstract theory of generating functions, but will instead content ourselves with an informal discussion and some examples. Informally, a generating function is an "object" that represents a counting function $f(i)$. Usually this object is a *formal power series*. The two most common types of generating functions are *ordinary* generating functions and *exponential* generating functions. If $I = \mathbb{N}$, then the ordinary generating function of $f(n)$ is the formal power series

$$\sum_{n\geq 0} f(n)x^n,$$

while the exponential generating function of $f(n)$ is the formal power series

$$\sum_{n\geq 0} f(n)\frac{x^n}{n!}.$$

(If $I = \mathbb{P}$, the positive integers, then these sums begin at $n = 1$.) These power series are called "formal" because we are not concerned with letting x take on particular values, and we ignore questions of convergence and divergence. The term x^n or $x^n/n!$ merely marks the place where $f(n)$ is written.

If $F(x) = \sum_{n\geq 0} a_n x^n$, then we call a_n the *coefficient* of x^n in $F(x)$ and write

$$a_n = [x^n]F(x).$$

Similarly, if $F(x) = \sum_{n\geq 0} a_n x^n/n!$, then we write

$$a_n = n![x^n]F(x).$$

In the same way we can deal with generating functions of several variables, such as

$$\sum_{l\geq 0}\sum_{m\geq 0}\sum_{n\geq 0} f(l,m,n)\frac{x^l y^m z^n}{n!}$$

(which may be considered as "ordinary" in the indices l, m and "exponential" in n), or even of infinitely many variables. In this latter case every term should involve only finitely many of the variables. A simple generating function in infinitely many variables is $x_1+x_2+x_3+\cdots$.

Why bother with generating functions if they are merely another way of writing a counting function? The answer is that we can perform various natural operations on generating functions that have a combinatorial significance. For instance, we can add two generating functions, say in one variable with $I = \mathbb{N}$, by the rule

$$\left(\sum_{n\geq 0} a_n x^n\right) + \left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0}(a_n + b_n)x^n$$

or

$$\left(\sum_{n\geq 0} a_n \frac{x^n}{n!}\right) + \left(\sum_{n\geq 0} b_n \frac{x^n}{n!}\right) = \sum_{n\geq 0}(a_n + b_n)\frac{x^n}{n!}.$$

Similarly, we can multiply generating functions according to the rule

$$\left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0} c_n x^n,$$

where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$, or

$$\left(\sum_{n\geq 0} a_n \frac{x^n}{n!}\right)\left(\sum_{n\geq 0} b_n \frac{x^n}{n!}\right) = \sum_{n\geq 0} d_n \frac{x^n}{n!},$$

where $d_n = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}$, with $\binom{n}{i} = n!/i!(n-i)!$. Note that these operations are just what we would obtain by treating generating functions as if they obeyed the ordinary laws of algebra, such as $x^i x^j = x^{i+j}$. These operations coincide with the addition and multiplication of functions when the power series converge for appropriate values of x, and they obey such familiar laws of algebra as associativity and commutativity of addition and multiplication, distributivity of multiplication over addition, and cancellation of multiplication (i.e., if $F(x)G(x) = F(x)H(x)$ and $F(x) \neq 0$, then $G(x) = H(x)$). In fact, the set of all formal power series $\sum_{n\geq 0} a_n x^n$ with complex coefficients a_n (or more generally, coefficients in any integral domain R, where integral domains are assumed to be commutative with a multiplicative identity 1) forms a (commutative) integral domain under the operations just defined. This integral domain is denoted $\mathbb{C}[[x]]$ (or more generally, $R[[x]]$). Actually, $\mathbb{C}[[x]]$, or more generally $K[[x]]$ when K is a field, is a very special type of integral domain. For readers with some familiarity with algebra, we remark that $\mathbb{C}[[x]]$ is a principal ideal domain and therefore a unique factorization domain. In fact, every ideal of $\mathbb{C}[[x]]$ has the form (x^n) for some $n \geq 0$. From the viewpoint of commutative algebra, $\mathbb{C}[[x]]$ is a one-dimensional complete regular local ring. Moreover, the operation $[x^n] : \mathbb{C}[[x]] \to \mathbb{C}$ of taking the coefficient of x^n (and similarly $[x^n/n!]$) is a linear functional on $\mathbb{C}[[x]]$. These general algebraic considerations will not concern us here; rather we will discuss from an elementary viewpoint the properties of $\mathbb{C}[[x]]$ that will be useful to us.

There is an obvious extension of the ring $\mathbb{C}[[x]]$ to formal power series in m variables $x_1, \ldots, x_m$. The set of all such power series with complex coefficients is denoted $\mathbb{C}[[x_1, \ldots, x_m]]$ and forms a unique factorization domain (though not a principal ideal domain for $m \geq 2$).

It is primarily through experience that the combinatorial significance of the algebraic operations of $\mathbb{C}[[x]]$ or $\mathbb{C}[[x_1, \ldots, x_m]]$ is understood, as well as the problems of whether to use ordinary or exponential generating functions (or various other kinds discussed in later chapters). In Section 3.18 we will explain to some extent the combinatorial significance of these operations, but even then experience is indispensable.

If $F(x)$ and $G(x)$ are elements of $\mathbb{C}[[x]]$ satisfying $F(x)G(x) = 1$, then we (naturally) write $G(x) = F(x)^{-1}$. (Here 1 is short for $1 + 0x + 0x^2 + \cdots$.) It is easy to see that $F(x)^{-1}$ exists (in which case it is unique) if and only if $a_0 \neq 0$, where $F(x) = \sum_{n \geq 0} a_n x^n$. One commonly writes "symbolically" $a_0 = F(0)$, even though $F(x)$ is not considered to be a function of x. If $F(0) \neq 0$ and $F(x)G(x) = H(x)$, then $G(x) = F(x)^{-1}H(x)$, which we also write as $G(x) = H(x)/F(x)$. More generally, the operation $^{-1}$ satisfies all the familiar laws of algebra, provided it is only applied to power series $F(x)$ satisfying $F(0) \neq 0$. For instance, $(F(x)G(x))^{-1} = F(x)^{-1}G(x)^{-1}$, $(F(x)^{-1})^{-1} = F(x)$, and so on. Similar results hold for $\mathbb{C}[[x_1, \ldots, x_m]]$.

1.1.5 Example. Let $\left(\sum_{n \geq 0} \alpha^n x^n\right)(1 - \alpha x) = \sum_{n \geq 0} c_n x^n$, where α is nonzero complex number. (We could also take α to be an indeterminate, in which case we should extend the coefficient field to $\mathbb{C}(\alpha)$, the field of rational functions over $\mathbb{C}$ in the variable α.) Then by definition of power series multiplication,

$$c_n = \begin{cases} 1, & n = 0 \\ \alpha^n - \alpha(\alpha^{n-1}) = 0, & n \geq 1. \end{cases}$$

Hence $\sum_{n \geq 0} \alpha^n x^n = (1 - \alpha x)^{-1}$, which can also be written

$$\sum_{n \geq 0} \alpha^n x^n = \frac{1}{1 - \alpha x}.$$

This formula comes as no surprise; it is simply the formula (in a formal setting) for summing a geometric series.

Example 1.1.5 provides a simple illustration of the general principle that, informally speaking, if we have an identity involving power series that is valid when the power series are regarded as functions (so that the variables are sufficiently small complex numbers), then this identity continues to remain valid when regarded as an identity among formal power series, *provided* the operations defined in the formulas are well-defined for formal power series. It would be unnecessarily pedantic for us to state a precise form of this principle here, since the reader should have little trouble justifying in any particular case the formal validity of our manipulations with power series. We will give several examples throughout this section to illustrate this contention.

1.1.6 Example. The identity

$$\left(\sum_{n\geq 0}\frac{x^n}{n!}\right)\left(\sum_{n\geq 0}(-1)^n\frac{x^n}{n!}\right)=1 \tag{1.3}$$

is valid at the function-theoretic level (it states that $e^x e^{-x}=1$) and is well-defined as a statement involving formal power series. Hence (1.3) is a valid formal power series identity. In other words (equating coefficients of $x^n/n!$ on both sides of (1.3)), we have

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}=\delta_{0n}. \tag{1.4}$$

To justify this identity directly from (1.3), we may reason as follows. Both sides of (1.3) converge for all $x\in\mathbb{C}$, so we have

$$\sum_{n\geq 0}\left(\sum_{k=0}^{n}(-1)^k\binom{n}{k}\right)\frac{x^n}{n!}=1, \qquad \text{for all } x\in\mathbb{C}.$$

But if two power series in x represent the same function $f(x)$ in a neighborhood of 0, then these two power series must agree term-by-term, by a standard elementary result concerning power series. Hence (1.4) follows.

1.1.7 Example. The identity

$$\sum_{n\geq 0}\frac{(x+1)^n}{n!}=e\sum_{n\geq 0}\frac{x^n}{n!}$$

is valid at the function-theoretic level (it states that $e^{x+1}=e\cdot e^x$), but does not make sense as a statement involving formal power series. There is no *formal* procedure for writing $\sum_{n\geq 0}(x+1)^n/n!$ as a member of $\mathbb{C}[[x]]$. For instance, the constant term of $\sum_{n\geq 0}(x+1)^n/n!$ is $\sum_{n\geq 0}1/n!$, whose interpretation as a member of $\mathbb{C}[[x]]$ involves the consideration of convergence.

Although the expression $\sum_{n\geq 0}(x+1)^n/n!$ does not make sense *formally*, there are nevertheless certain infinite processes that can be carried out formally in $\mathbb{C}[[x]]$. (These concepts extend straightforwardly to $\mathbb{C}[[x_1,\ldots,x_m]]$, but for simplicity we consider only $\mathbb{C}[[x]]$.) To define these processes, we need to put some additional structure on $\mathbb{C}[[x]]$—namely, the notion of *convergence*. From an algebraic standpoint, the definition of convergence is inherent in the statement that $\mathbb{C}[[x]]$ is *complete* in a certain standard topology that can be put on $\mathbb{C}[[x]]$. However, we will assume no knowledge of topology on the part of the reader and will instead give a self-contained, elementary treatment of convergence.

If $F_1(x),F_2(x),\ldots$ is a sequence of formal power series, and if $F(x)=\sum_{n\geq 0}a_n x^n$ is another formal power series, we say by definition that $F_i(x)$ *converges* to $F(x)$ as $i\to\infty$, written

$F_i(x) \to F(x)$ or $\lim_{i\to\infty} F_i(x) = F(x)$, provided that for all $n \geq 0$ there is a number $\delta(n)$ such that the coefficient of x^n in $F_i(x)$ is a_n whenever $i \geq \delta(n)$. In other words, for every n the sequence

$$[x^n]F_1(x),\ [x^n]F_2(x),\ \ldots$$

of complex numbers eventually becomes constant (or *stabilizes*) with value a_n. An equivalent definition of convergence is the following. Define the *degree* of a nonzero formal power series $F(x) = \sum_{n\geq 0} a_n x^n$, denoted $\deg F(x)$, to be the least integer n such that $a_n \neq 0$. Note that $\deg F(x)G(x) = \deg F(x) + \deg G(x)$. Then $F_i(x)$ converges if and only if $\lim_{i\to\infty} \deg(F_{i+1}(x) - F_i(x)) = \infty$, and $F_i(x)$ converges to $F(x)$ if and only if $\lim_{i\to\infty} \deg(F(x) - F_i(x)) = \infty$.

We now say that an infinite sum $\sum_{j\geq 0} F_j(x)$ has the value $F(x)$ provided that $\sum_{j=0}^{i} F_j(x) \to F(x)$. A similar definition is made for the infinite product $\prod_{j\geq 1} F_j(x)$. To avoid unimportant technicalities we assume that in any infinite product $\prod_{j\geq 1} F_j(x)$, each factor $F_j(x)$ satisfies $F_j(0) = 1$.

For instance, let $F_j(x) = a_j x^j$. Then for $i \geq n$, the coefficient of x^n in $\sum_{j=0}^{i} F_j(x)$ is a_n. Hence $\sum_{j\geq 0} F_j(x)$ is just the power series $\sum_{n\geq 0} a_n x^n$. Thus we can think of the formal power series $\sum_{n\geq 0} a_n x^n$ as actually being the "sum" of its individual terms. The proofs of the following two elementary results are left to the reader.

1.1.8 Proposition. The infinite series $\sum_{j\geq 0} F_j(x)$ converges if and only if

$$\lim_{j\to\infty} \deg F_j(x) = \infty.$$

1.1.9 Proposition. The infinite product $\prod_{j\geq 1}(1 + G_j(x))$, where $G_j(0) = 0$, converges if and only if $\lim_{j\to\infty} \deg G_j(x) = \infty$.

It is essential to realize that in evaluating a convergent series $\sum_{j\geq 0} F_j(x)$ (or similarly a product $\prod_{j\geq 1} F_j(x)$), the coefficient of x^n for any given n can be computed using only *finite* processes. For if j is sufficiently large, say $j > \delta(n)$, then $\deg F_j(x) > n$, so that

$$[x^n] \sum_{j\geq 0} F_j(x) = [x^n] \sum_{j=0}^{\delta(n)} F_j(x).$$

The latter expression involves only a *finite* sum.

The most important combinatorial application of the notion of convergence is to the idea of power series composition. If $F(x) = \sum_{n\geq 0} a_n x^n$ and $G(x)$ are formal power series with $G(0) = 0$, define the *composition* $F(G(x))$ to be the infinite sum $\sum_{n\geq 0} a_n G(x)^n$. Since $\deg G(x)^n = n \cdot \deg G(x) \geq n$, we see by Proposition 1.1.8 that $F(G(x))$ is well-defined as a *formal* power series. We also see why an expression such as e^{1+x} does not make sense formally; namely, the infinite series $\sum_{n\geq 0}(1+x)^n/n!$ does not converge in accordance with the above definition. On the other hand, an expression like e^{e^x-1} makes good sense formally, since it has the form $F(G(x))$ where $F(x) = \sum_{n\geq 0} x^n/n!$ and $G(x) = \sum_{n\geq 1} x^n/n!$.

1.1.10 Example. If $F(x) \in \mathbb{C}[[x]]$ satisfies $F(0) = 0$, then we can *define* for any $\lambda \in \mathbb{C}$ the formal power series

$$(1 + F(x))^\lambda = \sum_{n \geq 0} \binom{\lambda}{n} F(x)^n, \tag{1.5}$$

where $\binom{\lambda}{n} = \lambda(\lambda - 1) \cdots (\lambda - n + 1)/n!$. In fact, we may regard λ as an indeterminate and take (1.5) as the definition of $(1 + F(x))^\lambda$ as an element of $\mathbb{C}[[x, \lambda]]$ (or of $\mathbb{C}[\lambda][[x]]$; that is, the coefficient of x^n in $(1 + F(x))^\lambda$ is a certain *polynomial* in λ). All the expected properties of exponentiation are indeed valid, such as

$$(1 + F(x))^{\lambda+\mu} = (1 + F(x))^\lambda (1 + F(x))^\mu,$$

regarded as an identity in the ring $\mathbb{C}[[x, \lambda, \mu]]$, or in the ring $\mathbb{C}[[x]]$ where one takes $\lambda, \mu \in \mathbb{C}$.

If $F(x) = \sum_{n \geq 0} a_n x^n$, define the *formal derivative* $F'(x)$ (also denoted $\frac{dF}{dx}$ or $DF(x)$) to be the formal power series

$$F'(x) = \sum_{n \geq 0} n a_n x^{n-1} = \sum_{n \geq 0} (n + 1) a_{n+1} x^n.$$

It is easy to check that all the familiar laws of differentiation that are well-defined formally continue to be valid for formal power series, In particular,

$$\begin{aligned} (F + G)' &= F' + G' \\ (FG)' &= F'G + FG' \\ F(G(x))' &= G'(x)F'(G(x)). \end{aligned}$$

We thus have a theory of *formal calculus* for formal power series. The usefulness of this theory will become apparent in subsequent examples. We first give an example of the use of the formal calculus that should shed some additional light on the validity of manipulating formal power series $F(x)$ as if they were actual functions of x.

1.1.11 Example. Suppose $F(0) = 1$, and let $G(x)$ be the power series (easily seen to be unique) satisfying

$$G'(x) = F'(x)/F(x), \qquad G(0) = 0. \tag{1.6}$$

From the function-theoretic viewpoint we can "solve" (1.6) to obtain $F(x) = \exp G(x)$, where by definition

$$\exp G(x) = \sum_{n \geq 0} \frac{G(x)^n}{n!}.$$

Since $G(0) = 0$ everything is well-defined formally, so (1.6) should remain equivalent to $F(x) = \exp G(x)$ even if the power series for $F(x)$ converges only at $x = 0$. How can this assertion be justified without actually proving a combinatorial identity? Let $F(x) = 1 + \sum_{n \geq 1} a_n x^n$. From (1.6) we can compute explicitly $G(x) = \sum_{n \geq 1} b_n x^n$, and it is quickly seen that each b_n is a *polynomial* in finitely many of the a_i's. It then follows that if $\exp G(x) = 1 + \sum_{n \geq 1} c_n x^n$, then each c_n will also be a polynomial in finitely many of the a_i's, say

$c_n = p_n(a_1, a_2, \ldots, a_m)$, where m depends on n. Now we know that $F(x) = \exp G(x)$ provided $1 + \sum_{n\geq 1} a_n x^n$ converges. If two Taylor series convergent in some neighborhood of the origin represent the same function, then their coefficients coincide. Hence $a_n = p_n(a_1, a_2, \ldots, a_m)$ provided $1 + \sum_{n\geq 1} a_n x^n$ converges. Thus the two polynomials a_n and $p_n(a_1, \ldots, a_m)$ agree in some neighborhood of the origin of $\mathbb{C}^m$, so they must be equal. (It is a simple result that if two complex polynomials in m variables agree in some open subset of $\mathbb{C}^m$, then they are identical.) Since $a_n = p_n(a_1, a_2, \ldots, a_m)$ as polynomials, the identity $F(x) = \exp G(x)$ continues to remain valid for *formal* power series.

There is an alternative method for justifying the formal solution $F(x) = \exp G(x)$ to (1.6), which may appeal to topologically inclined readers. Given $G(x)$ with $G(0) = 0$, define $F(x) = \exp G(x)$ and consider a map $\phi : \mathbb{C}[[x]] \to \mathbb{C}[[x]]$ defined by $\phi(G(x)) = G'(x) - \frac{F'(x)}{F(x)}$. One easily verifies the following: (a) if G converges in some neighborhood of 0 then $\phi(G(x)) = 0$; (b) the set $\mathcal{G}$ of all power series $G(x) \in \mathbb{C}[[x]]$ that converge in some neighborhood of 0 is dense in $\mathbb{C}[[x]]$, in the topology defined above (in fact, the set $\mathbb{C}[x]$ of polynomials is dense); and (c) the function ϕ is continuous in the topology defined above. From this it follows that $\phi(G(x)) = 0$ for all $G(x) \in \mathbb{C}[[x]]$ with $G(0) = 0$.

We now present various illustrations in the manipulation of generating functions. Throughout we will be making heavy use of the principle that formal power series can be treated as if they were functions.

1.1.12 Example. Find a simple expression for the generating function $F(x) = \sum_{n\geq 0} a_n x^n$, where $a_0 = a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$ if $n \geq 2$. We have

$$\begin{aligned} F(x) &= \sum_{n\geq 0} a_n x^n = 1 + x + \sum_{n\geq 2} a_n x^n \\ &= 1 + x + \sum_{n\geq 2} (a_{n-1} + a_{n-2}) x^n \\ &= 1 + x + x \sum_{n\geq 2} a_{n-1} x^{n-1} + x^2 \sum_{n\geq 2} a_{n-2} x^{n-2} \\ &= 1 + x + x(F(x) - 1) + x^2 F(x). \end{aligned}$$

Solving for $F(x)$ yields $F(x) = 1/(1 - x - x^2)$. The number a_n is just the *Fibonacci number* F_{n+1}. For some combinatorial properties of Fibonacci numbers, see Exercises 1.35–1.42. For the general theory of rational generating functions and linear recurrences with constant coefficients illustrated in the present example, see Section 4.1.

1.1.13 Example. Find a simple expression for the generating function $F(x) = \sum_{n\geq 0} a_n x^n/n!$, where $a_0 = 1$,

$$a_{n+1} = a_n + n a_{n-1}, \quad n \geq 0. \tag{1.7}$$

(Note that if $n = 0$ we get $a_1 = a_0 + 0 \cdot a_{-1}$, so the value of a_{-1} is irrelevant.) Multiply the

recurrence (1.7) by $x^n/n!$ and sum on $n \geq 0$. We get

$$\begin{aligned}\sum_{n\geq 0} a_{n+1}\frac{x^n}{n!} &= \sum_{n\geq 0} a_n \frac{x^n}{n!} + \sum_{n\geq 0} n a_{n-1}\frac{x^n}{n!} \\ &= \sum_{n\geq 0} a_n \frac{x^n}{n!} + \sum_{n\geq 1} a_{n-1}\frac{x^n}{(n-1)!}.\end{aligned}$$

The left-hand side is just $F'(x)$, while the right-hand side is $F(x) + xF(x)$. Hence $F'(x) = (1+x)F(x)$. The unique solution to this differential equation satisfying $F(0) = 1$ is $F(x) = \exp\left(x + \frac{1}{2}x^2\right)$. (As shown in Example 1.1.11, solving this differential equation is a purely formal procedure.) For the combinatorial significance of the numbers a_n, see equation (5.32).

NOTE. With the benefit of hindsight we wrote the recurrence $a_{n+1} = a_n + na_{n-1}$ with indexing that makes the computation simplest. If for instance we had written $a_n = a_{n-1} + (n-1)a_{n-2}$, then the computation would be more complicated (though still quite tractable). In converting recurrences to generating function identities, it can be worthwhile to consider how best to index the recurrence.

1.1.14 Example. Let $\mu(n)$ be the Möbius function of number theory; that is, $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by the square of an integer greater than one, and $\mu(n) = (-1)^r$ if n is the product of r distinct primes. Find a simple expression for the power series

$$F(x) = \prod_{n\geq 1}(1-x^n)^{-\mu(n)/n}. \tag{1.8}$$

First let us make sure that $F(x)$ is well-defined as a formal power series. We have by Example 1.1.10 that

$$(1-x^n)^{-\mu(n)/n} = \sum_{i\geq 0}\binom{-\mu(n)/n}{i}(-1)^i x^{in}.$$

Note that $(1-x^n)^{-\mu(n)/n} = 1 + H(x)$, where $\deg H(x) = n$. Hence by Proposition 1.1.9 the infinite product (1.8) converges, so $F(x)$ is well-defined. Now apply log to (1.8). In other words, form $\log F(x)$, where

$$\log(1+x) = \sum_{n\geq 1}(-1)^{n-1}\frac{x^n}{n},$$

the power series expansion for the natural logarithm at $x = 0$. We obtain

$$\begin{aligned}\log F(x) &= \log \prod_{n\geq 1}(1-x^n)^{-\mu(n)/n} \\ &= -\sum_{n\geq 1}\log(1-x^n)^{\mu(n)/n} \\ &= -\sum_{n\geq 1}\frac{\mu(n)}{n}\log(1-x^n) \\ &= -\sum_{n\geq 1}\frac{\mu(n)}{n}\sum_{i\geq 1}\left(-\frac{x^{in}}{i}\right).\end{aligned}$$

The coefficient of x^m in the above power series is

$$\frac{1}{m}\sum_{d|m}\mu(d),$$

where the sum is over all positive integers d dividing m. It is well-known that

$$\frac{1}{m}\sum_{d|m}\mu(d) = \begin{cases} 1, & m = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Hence $\log F(x) = x$, so $F(x) = e^x$. Note that the derivation of this miraculous formula involved only *formal* manipulations.

1.1.15 Example. Find the unique sequence $a_0 = 1, a_1, a_2, \ldots$ of real numbers satisfying

$$\sum_{k=0}^{n} a_k a_{n-k} = 1 \tag{1.9}$$

for all $n \in \mathbb{N}$. The trick is to recognize the left-hand side of (1.9) as the coefficient of x^n in $\left(\sum_{n\geq 0} a_n x^n\right)^2$. Letting $F(x) = \sum_{n\geq 0} a_n x^n$, we then have

$$F(x)^2 = \sum_{n\geq 0} x^n = \frac{1}{1-x}.$$

Hence

$$F(x) = (1-x)^{-1/2} = \sum_{n\geq 0} \binom{-1/2}{n} (-1)^n x^n,$$

so

$$\begin{aligned} a_n &= (-1)^n \binom{-1/2}{n} \\ &= (-1)^n \frac{\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)\cdots\left(-\frac{2n-1}{2}\right)}{n!} \\ &= \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n n!}. \end{aligned}$$

Note that a_n can also be rewritten as $4^{-n}\binom{2n}{n}$. The identity

$$\binom{2n}{n} = (-1)^n 4^n \binom{-1/2}{n} \tag{1.10}$$

can be useful for problems involving $\binom{2n}{n}$.

Now that we have discussed the manipulation of formal power series, the question arises as to the advantages of using generating functions to represent a counting function $f(n)$. Why, for instance, should a formula such as

$$\sum_{n\geq 0} f(n)\frac{x^n}{n!} = \exp\left(x + \frac{x^2}{2}\right) \tag{1.11}$$

be regarded as a "determination" of $f(n)$? Basically, the answer is that there are many standard, routine techniques for extracting information from generating functions. Generating functions are frequently the most concise and efficient way of presenting information about their coefficients. For instance, from (1.11) an experienced enumerative combinatorialist can tell at a glance the following:

1. A simple recurrence for $f(n)$ can be found by differentiation. Namely, we obtain

$$\sum_{n\geq 1} f(n)\frac{x^{n-1}}{(n-1)!} = (1+x)e^{x+x^2/2} = (1+x)\sum_{n\geq 0} f(n)\frac{x^n}{n!}.$$

Equating coefficients of $x^n/n!$ yields

$$f(n+1) = f(n) + nf(n-1), \quad n \geq 1.$$

Note that in Example 1.1.13 we went in the opposite direction, i.e., we obtained the generating function from the recurrence, a less straightforward procedure.

2. An explicit formula for $f(n)$ can be obtained from $e^{x+(x^2/2)} = e^x e^{x^2/2}$. Namely,

$$\begin{aligned}\sum_{n\geq 0} f(n)\frac{x^n}{n!} &= e^x e^{x^2/2} = \left(\sum_{n\geq 0}\frac{x^n}{n!}\right)\left(\sum_{n\geq 0}\frac{x^{2n}}{2^n n!}\right)\\ &= \left(\sum_{n\geq 0}\frac{x^n}{n!}\right)\left(\sum_{n\geq 0}\frac{(2n)!}{2^n n!}\frac{x^{2n}}{(2n)!}\right),\end{aligned}$$

so that

$$f(n) = \sum_{\substack{i\geq 0\\ i \text{ even}}} \binom{n}{i}\frac{i!}{2^{i/2}(i/2)!} = \sum_{j\geq 0}\binom{n}{2j}\frac{(2j)!}{2^j j!}.$$

3. Regarded as a function of a complex variable, $\exp\left(x + \frac{x^2}{2}\right)$ is a nicely behaved entire function, so that standard techniques from the theory of asymptotic analysis can be used to estimate $f(n)$. As a first approximation, it is routine (for someone sufficiently versed in complex variable theory) to obtain the asymptotic formula

$$f(n) \sim \frac{1}{\sqrt{2}} n^{n/2} e^{-\frac{n}{2}+\sqrt{n}-\frac{1}{4}}. \tag{1.12}$$

No other method of describing $f(n)$ makes it so easy to determine these fundamental properties. Many other properties of $f(n)$ can also be easily obtained from the generating function;

for instance, we leave to the reader the problem of evaluating, essentially by inspection of (1.11), the sum

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}f(i) \tag{1.13}$$

(see Exercise 1.7). Therefore we are ready to accept the generating function $\exp\left(x+\frac{x^2}{2}\right)$ as a satisfactory determination of $f(n)$.

This completes our discussion of generating functions and more generally the problem of giving a satisfactory description of a counting function $f(n)$. We now turn to the question of what is the best way to *prove* that a counting function has some given description. In accordance with the principle from other branches of mathematics that it is better to exhibit an explicit isomorphism between two objects than merely prove that they are isomorphic, we adopt the general principle that it is better to exhibit an explicit one-to-one correspondence (bijection) between two finite sets than merely to prove that they have the same number of elements. A proof that shows that a certain set S has a certain number m of elements by constructing an explicit bijection between S and some other set that is known to have m elements is called a *combinatorial proof* or *bijective proof*. The precise border between combinatorial and non-combinatorial proofs is rather hazy, and certain arguments that to an inexperienced enumerator will appear non-combinatorial will be recognized by a more facile counter as combinatorial, primarily because he or she is aware of certain standard techniques for converting apparently non-combinatorial arguments into combinatorial ones. Such subtleties will not concern us here, and we now give some clear-cut examples of the distinction between combinatorial and non-combinatorial proofs. We use the notation $\#S$ or $|S|$ for the cardinality (number of elements) of the finite set S.

1.1.16 Example. Let n and k be fixed positive integers. How many sequences $(X_1, X_2, \ldots, X_k)$ are there of subsets of the set $[n] = \{1, 2, \ldots, n\}$ such that $X_1 \cap X_2 \cap \cdots \cap X_k = \emptyset$? Let $f(k, n)$ be this number. If we were not particularly inspired we could perhaps argue as follows. Suppose $X_1 \cap X_2 \cap \cdots \cap X_{k-1} = T$, where $\#T = i$. If $Y_j = X_j - T$, then $Y_1 \cap \cdots \cap Y_{k-1} = \emptyset$ and $Y_j \subseteq [n] - T$. Hence there are $f(k-1, n-i)$ sequences $(X_1, \ldots, X_{k-1})$ such that $X_1 \cap X_2 \cap \cdots \cap X_{k-1} = T$. For each such sequence, X_k can be any of the 2^{n-i} subsets of $[n] - T$. As is probably familiar to most readers and will be discussed later, there are $\binom{n}{i} = n!/i!(n-i)!$ i-element subsets T of $[n]$. Hence

$$f(k,n) = \sum_{i=0}^{n}\binom{n}{i}2^{n-i}f(k-1,n-i). \tag{1.14}$$

Let $F_k(x) = \sum_{n\geq 0} f(k,n)x^n/n!$. Then (1.14) is equivalent to

$$F_k(x) = e^x F_{k-1}(2x).$$

Clearly $F_1(x) = e^x$. It follows easily that

$$\begin{aligned} F_k(x) &= \exp(x + 2x + 4x + \cdots + 2^{k-1}x) \\ &= \exp((2^k - 1)x) \\ &= \sum_{n\geq 0}(2^k-1)^n\frac{x^n}{n!}. \end{aligned}$$

Hence $f(k,n) = (2^k-1)^n$. This argument is a flagrant example of a non-combinatorial proof. The resulting answer is extremely simple despite the contortions involved to obtain it, and it cries out for a better understanding. In fact, $(2^k-1)^n$ is clearly the number of n-tuples $(Z_1, Z_2, \ldots, Z_n)$, where each Z_i is a subset of $[k]$ not equal to $[k]$. Can we find a bijection θ between the set S_{kn} of all $(X_1, \ldots, X_k) \subseteq [n]^k$ such that $X_1 \cap \cdots \cap X_k = \emptyset$, and the set T_{kn} of all $(Z_1, \ldots, Z_n)$ where $[k] \neq Z_i \subseteq [k]$? Given an element $(Z_1, \ldots, Z_n)$ of T_{kn}, define $(X_1, \ldots, X_k)$ by the condition that $i \in X_j$ if and only if $j \in Z_i$. This rule is just a precise way of saying the following: the element 1 can appear in any of the X_i's except all of them, so there are $2^k - 1$ choices for which of the X_i's contain 1; similarly there are $2^k - 1$ choices for which of the X_i's contain $2, 3, \ldots, n$, so there are $(2^k-1)^n$ choices in all. Thus the crucial point of the problem is that the different elements of $[n]$ behave *independently*, so we end up with a simple product. We leave to the reader the (rather dull) task of rigorously verifiying that θ is a bijection, but this fact should be intuitively clear. The usual way to show that θ is a bijection is to construct explicitly a map $\phi : T_{kn} \to S_{kn}$, and then to show that $\phi = \theta^{-1}$; for example, by showing that $\phi\theta(X) = X$ and that θ is surjective. *Caveat*: any proof that θ is bijective must not use a priori the fact that $\#S_{kn} = \#T_{kn}$!

Not only is the above combinatorial proof much shorter than our previous proof, but it also makes the reason for the simple answer completely transparent. It is often the case, as occurred here, that the first proof to come to mind turns out to be laborious and inelegant, but that the final answer suggests a simpler combinatorial proof.

1.1.17 Example. Verify the identity

$$\sum_{i=0}^{n} \binom{a}{i}\binom{b}{n-i} = \binom{a+b}{n}, \tag{1.15}$$

where a, b, and n are nonnegative integers. A non-combinatorial proof would run as follows. The left-hand side of (1.15) is the coefficient of x^n in the power series (polynomial) $\left(\sum_{i\geq 0}\binom{a}{i}x^i\right)\left(\sum_{j\geq 0}\binom{b}{j}x^j\right)$. But by the binomial theorem,

$$\begin{aligned}\left(\sum_{i\geq 0}\binom{a}{i}x^i\right)\left(\sum_{j\geq 0}\binom{b}{j}x^j\right) &= (1+x)^a(1+x)^b \\ &= (1+x)^{a+b} \\ &= \sum_{n\geq 0}\binom{a+b}{n}x^n,\end{aligned}$$

so the proof follows. A combinatorial proof runs as follows. The right-hand side of (1.15) is the number of n-element subsets X of $[a+b]$. Suppose X intersects $[a]$ in i elements. There are $\binom{a}{i}$ choices for $X \cap [a]$, and $\binom{b}{n-i}$ choices for the remaining $n-i$ elements $X \cap \{a+1, a+2, \ldots, a+b\}$. Thus there are $\binom{a}{i}\binom{b}{n-i}$ ways that $X \cap [a]$ can have i elements, and summing over i gives the total number $\binom{a+b}{n}$ of n-element subsets of $[a+b]$.

There are many examples in the literature of finite sets that are known to have the same number of elements but for which no combinatorial proof of this fact is known. Some of these will appear as exercises throughout this book.