

Lecture notes for “Enumerative Combinatorics”

Anna de Mier*
University of Oxford

Michaelmas Term 2004[†]

Contents

1	Subsets, multisets, and balls-in-bins	3
1.1	Words and permutations	3
1.2	Subsets and binomial numbers	4
1.3	Multisets and integer compositions	7
1.4	Balls-and-bins and multinomial numbers	9
1.5	Mappings	10
2	The Principle of Inclusion and Exclusion	10
3	Integer and set partitions; Stirling numbers	14
3.1	Integer partitions	14
3.2	Set partitions	17
3.3	Decomposition of permutations into disjoint cycles	19
4	Generating functions and recurrences	20
4.1	Formal power series	24
4.2	Linear recurrences	26
4.3	A non-linear recurrence: Catalan numbers	29
4.4	The generating function for integer partitions	31

*Please e-mail any comments or suggestions to ademier@gmail.com; thanks to the ones that have already done it.

[†]Last correction: 15 June 2006.

5	The symbolic method for unlabelled structures	33
5.1	Constructions	34
5.2	Compositions revisited	38
5.3	Rooted plane trees	39
6	The symbolic method for labelled structures	41
6.1	Constructions	42
6.2	Labelled graphs	45
6.3	Set partitions revisited	46
6.4	Permutation decompositions revisited	47

A good way to convey what an area of Mathematics is about is by giving a list of problems. This is particularly true in Combinatorics. In this course, we attempt to solve problems like:

In how many ways...

- can we pick 6 numbers from 1 to 15 so that no two are consecutive?
- can we climb a ladder if we move up either one or two steps at a time?
- can 7 balls be placed in 4 boxes if no box is to be left empty?
- can we give change of a pound?

As suggested by the title of the course, we will be mainly concerned with counting problems, although on our way we will encounter algebraic and structural questions. The first thing we learn about maths is to count, but as we shall see counting can become quite tricky and requires techniques.

The course has two parts. The first one introduces the basic objects, ideas, and principles in enumeration. The second part is devoted to generating functions and their powerful uses. The beginning of the course is sort of “linear”, since we will describe a good variety of relatively simple objects; but those are not to be forgotten, since as we go our way into the subject they will appear once and again under new lights and perspectives. Enumeration is better understood by example; for this reason, we encourage visual and combinatorial proofs, and the examples treated should be used as inspiration to solve further problems.

Notation. Unless otherwise stated, all sets considered will be finite; an n -set is a set with n elements; a k -subset of a set is a subset with k elements. The set of the first n integers, that is $\{1, 2, 3, \dots, n\}$, will be denoted by $[n]$.

1 Subsets, multisets, and balls-in-bins

This chapter deals with choice problems that might be familiar from probability courses; they are sometimes called “combinations” and “variations”, with or without “repetition”. In this course we do not use this notation and we only refer to counting permutations, subsets, multisets, etc...

1.1 Words and permutations

Let us start by looking at a very simple object.

Definition 1.1. A word over the alphabet X is a finite sequence of elements of X .

Example. Some words over the alphabet $[5]$ are 123, 231, 125, 435, 443, ...

Theorem 1.2. There are n^k words of length k over an alphabet of n symbols.

Proof. We have n choices for the first letter, n choices for the second letter, and so on, until we have n choices for the last letter. Hence, there are $n \cdot n \cdots n = n^k$ words of length k . \square

Words allow symbols to be repeated. Permutations are sequences where all elements are different.

Definition 1.3. A permutation of a set X is a total linear ordering of the elements of X ; we represent it as $x_1x_2 \cdots x_n$.

Example. The set $[3]$ has 6 permutations: 123, 132, 213, 231, 312, 321.

Theorem 1.4. The number of permutations of an n -element set X is $n!$.

Proof. We have n choices for the first element x_1 . Once this is chosen, we have $n-1$ choices for x_2 ; then, $n-2$ choices for x_3 , and so on, until we have only one choice for the last element x_n . Therefore the total number of permutations of X is $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$. \square

Definition 1.5. A k -permutation of a set X is a total linear ordering of a k -subset of X ; we represent it as $x_1x_2 \cdots x_k$.

Example. The set $[3]$ also has 6 2-permutations: 12, 13, 21, 23, 31, 32, but it only has 3 1-permutations: 1, 2, 3.

Theorem 1.6. An n -set X has $\frac{n!}{(n-k)!} = n(n-1) \cdots (n-k+1)$ k -permutations.

Proof. We proceed as in the proof of Theorem 1.4. There are n choices for x_1 , $n-1$ choices for x_2 , and so on, until we have $n-k+1$ choices for x_k . \square

The set of all permutations of X is denoted \mathcal{S}_X ; if $X = [n]$, we simplify to the usual notation from group theory: \mathcal{S}_n . Permutations can not only be viewed as arrangements of elements, but also as bijective maps from $[n]$ onto X . If π is the permutation $x_1x_2 \cdots x_n$, it defines also a map $\pi : [n] \rightarrow X$ as $\pi(i) = x_i$. The group \mathcal{S}_n has a particularly rich structure that has been extensively studied; the algebraic point of view does not have an important role for our purposes, but some basic results on representing permutations as products of cycles will be needed later in the course.

1.2 Subsets and binomial numbers

This section is concerned with the number of ways in which we can select a k -element subset of an n -set (regardless of the order of the elements, in opposition to permutations). We start by examining some properties of this number and later we derive a formula for it.

Definition 1.7. $\binom{n}{k}$ denotes the number of subsets of size k of $[n]$; or, equivalently, the number of ways in which we can select k different elements from an n -element set.

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Table 1: Pascal's Triangle.

The number $\binom{n}{k}$ is read “ n choose k ” and is called a *binomial number* or a *binomial coefficient*.

We start with some basic properties of binomial numbers. The first three follow directly from the definition.

- (1) $\binom{n}{0} = \binom{n}{n} = 1$
- (2) $\binom{n}{1} = \binom{n}{n-1} = n$
- (3) $\binom{n}{k} = \binom{n}{n-k}$

The following is the key recurrence relation for binomial numbers.

$$(4) \quad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \text{ for } n > k \geq 1$$

Proof. We prove this equality by counting subsets of $[n]$ according to whether or not they include a fixed element, say n . Let A be a k -subset of $[n]$; in total there are $\binom{n}{k}$ ways of choosing A . If A does not include the element n , then A can be chosen in $\binom{n-1}{k}$ ways; on the other hand, if A does contain n , then the remaining $k-1$ elements of A can be chosen from $[n-1]$ in $\binom{n-1}{k-1}$ ways. \square

The proof above is an example of what is called a *combinatorial* proof, in contrast to *algebraic* proofs. It is often the case that a result can be proved in a variety of ways, some of them using algebraic tools, some others based on bijections or on structural properties. Of course all proofs are correct and valid, although in general combinatorial proofs tend to be more beautiful and enlightening (and sometimes quite difficult to find!).

Recurrence (4) allows us to compute binomial numbers recursively; table 1 is usually called *Pascal's triangle*. In further sections we will encounter other combinatorial numbers that satisfy similar relations that are proved using analogous ideas.

The following is Newton's famous Binomial Theorem (from which binomial numbers take their name).

Theorem 1.8. (Binomial Theorem) For all integers $n \geq 0$,

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

Proof. Write $(a + b)^n$ as $(a + b)(a + b) \cdots (a + b)$. To expand this product we have to choose either an a or a b from each of the factors $(a + b)$. Hence each term in the expansion is of the form $a^k b^{n-k}$ for some k between 0 and n . This term will appear as many times as ways of picking k a 's from the product above; this is the same as selecting k of the n factors $(a + b)$, and this can be done in $\binom{n}{k}$ ways. Hence the coefficient of $a^k b^{n-k}$ in the binomial is $\binom{n}{k}$. \square

As an application of the binomial theorem, we prove the following summation formulas for binomial coefficients.

$$(5) \sum_{k=0}^n \binom{n}{k} = 2^n$$

$$(6) \sum_{k=0}^n (-1)^k \binom{n}{k} = 0$$

Proof. By the binomial theorem,

$$\sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = (1 + 1)^n = 2^n,$$

and

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

\square

This proof is an archetypical example of an *algebraic proof*; the meaning of $\binom{n}{k}$ plays no role, only its algebraic properties. Equality (5) is equivalent to saying that the total number of subsets of an n -set is 2^n . If X is a set, we denote by $\mathcal{P}(X)$ the set of all subsets of X (including \emptyset and X). Hence, we have just proved that $|\mathcal{P}(X)| = 2^{|X|}$. Equality (6) above can be phrased as “the number of subsets of even size of an n -set equals the number of subsets of odd size”. Can you find combinatorial proofs for these equalities?

Finally we come to the well-known formula for binomial numbers. (By definition, $0! = 1$.)

Theorem 1.9.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad \text{for } n \geq k \geq 0.$$

Proof. A k -subset of an n -set can be seen as a k -permutation in which the order of the elements does not matter. Hence, to pick a k -subset, just pick a k -permutation and forget

about the order of the elements. Since there are $n!/(n-k)!$ k -permutations and a set of size k can be ordered in $k!$ ways, we have that the total number of k -subsets of an n -set is

$$\frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{k!(n-k)!}.$$

□

1.3 Multisets and integer compositions

Up to now we have only considered the case of selecting distinct elements of a set (with or without order). The next step is to allow repetitions in the elements we select. Towards this end we have to introduce the concept of a multiset; a multiset is like a set, but we allow each element to be repeated a (finite) number of times.

Definition 1.10. Let X be a set. A multiset M on X is a function $\nu : X \rightarrow \mathbb{N}$ such that $\nu(x)$ is finite for all $x \in X$. The number $\nu(x)$ is the number of copies (or repetitions) of x , and $\sum_{x \in X} \nu(x)$ is the size of M .

Example. Let $X = \{a, b, c, d\}$. The multiset corresponding to the function

$$\nu(a) = 2 \quad \nu(b) = 0 \quad \nu(c) = 1 \quad \nu(d) = 3$$

can be represented as $\{a, a, c, d, d, d\}$. The size of M is 6.

We now count how many multisets of size k does an n -set have. In other words, in how many ways we can pick k elements from an n -set if we can repeat elements.

Let x_1, \dots, x_n be the elements of X . To select a multiset of size k we have to select non-negative numbers a_1, \dots, a_n such that $a_1 + \dots + a_n = k$. Here, a_i is the number of copies of x_i we pick.

Theorem 1.11. The number of solutions to the equation

$$a_1 + \dots + a_n = k, \quad a_i \geq 0, a_i \in \mathbb{N},$$

is $\binom{k+n-1}{k}$. In other words, an n -set has $\binom{k+n-1}{k}$ multisets of size k .

Proof. The problem is the same as finding the number of ways of placing k undistinguishable balls in n numbered boxes (a_i represents then the number of balls in box i). Put the k balls in a row.

• • • • •

To represent the boxes we use vertical bars $|$, meaning the separation between two consecutive boxes. Hence we need $n-1$ bars. A distribution of the balls in the boxes is then an arrangement of bars and balls, such as

• || • • | • • • • • |

In this arrangement we have five boxes, of which the first has one ball, the second and the last ones are empty, the third has two balls, and the fourth has six balls. So, in total we

have $k + n - 1$ positions that can be either \bullet or $|$, and k of the positions are \bullet . Since there is no further restriction, the solution is the number of ways of selecting k elements from a set of $k + n - 1$, and therefore the theorem follows. \square

Multisets are strongly related to integer compositions.

Definition 1.12. A composition of an integer n is an expression of n as an ordered sum $n = n_1 + n_2 + \cdots + n_k$ of strictly positive integers.

Example. Let us find all compositions of the first integers.

$$\begin{aligned} 1 \\ 2 &= 1 + 1 \\ 3 &= 2 + 1 = 1 + 2 = 1 + 1 + 1 \\ 4 &= 3 + 1 = 1 + 3 = 2 + 2 = 2 + 1 + 1 = 1 + 2 + 1 = 1 + 1 + 2 = 1 + 1 + 1 + 1 \end{aligned}$$

Let $c(n)$ be the number of compositions of the integer n and let $c_k(n)$ be the number of compositions of n in exactly k parts. The example above suggests that $c(n) = 2^{n-1}$. We shall prove this by finding first a formula for $c_k(n)$.

Theorem 1.13. The number of compositions of n in k parts is $c_k(n) = \binom{n-1}{k-1}$.

The total number of compositions of n is 2^{n-1} .

Proof. Observe that $c_k(n)$ is the number of solutions to the equation $n_1 + \cdots + n_k = n$ with $n_i \geq 1$. We proceed as in the proof of Theorem 1.11: we have to distribute n balls in k boxes, but now no box can be left empty. In terms of the balls and bars diagram, we have n balls \bullet and $k - 1$ separations $|$ with the extra condition that no two bars can be consecutive. Hence, between any two consecutive \bullet we can place at most one $|$. Hence, from the $n - 1$ spaces between two \bullet we have to select $k - 1$ to put a $|$. This can be done in $\binom{n-1}{k-1}$ ways.

The formula for $c(n)$ is found by summing all the $c_k(n)$ and applying the binomial theorem.

$$c(n) = c_1(n) + c_2(n) + \cdots + c_n(n) = \sum_{k=1}^n \binom{n-1}{k-1} = \sum_{j=0}^{n-1} \binom{n-1}{j} = 2^{n-1}$$

\square

Our proof for the formula $c(n) = 2^{n-1}$ is again algebraic, but there are also combinatorial proofs. Try to find one (there are several, but one follows nicely using balls and bars diagrams as above).

1.4 Balls-and-bins and multinomial numbers

Suppose we have m numbered balls that we want to place in r numbered bins. In how many ways can this be done if we do not impose any extra condition?

We have r choices for where to put ball 1; for ball 2 we have again r choices; and again r choices for each of the balls 3 to m . Hence, in total we have $r \cdot r \cdots r = r^m$ possibilities.

Now suppose that we are given the number of balls that must go into each of the bins, that is, we have numbers m_1, \dots, m_r so that bin i has to contain m_i balls. (Implicit in the definition is that $m_1 + m_2 + \cdots + m_r = m$.)

Let us count the number of ways of placing the balls by counting the number of possibilities for each bin. In bin 1 we have to put m_1 balls, so there are $\binom{m}{m_1}$ choices. Bin 2 must contain m_2 balls, but of course we cannot choose among the ones that we have already put in bin 1. Hence, there are $\binom{m-m_1}{m_2}$ choices. Similarly, we have $\binom{m-m_1-m_2}{m_3}$ choices for bin 3, and so on, until the last bin. Thus the number of ways of placing m balls in r bins with m_i balls in bin i is

$$\begin{aligned} & \binom{m}{m_1} \binom{m-m_1}{m_2} \binom{m-m_1-m_2}{m_3} \cdots \binom{m-m_1-\cdots-m_{r-1}}{m_r} = \\ & \frac{m!}{m_1!(m-m_1)!} \frac{(m-m_1)!}{m_2!(m-m_1-m_2)!} \frac{(m-m_1-m_2)!}{m_3!(m-m_1-m_2-m_3)!} \cdots \frac{(m-m_1-\cdots-m_{r-1})!}{m_r!0!} = \\ & \frac{m!}{m_1!m_2! \cdots m_r!}. \end{aligned}$$

This number is denoted by $\binom{m}{m_1, m_2, \dots, m_r}$ and it is called a *multinomial number*. Notice that when $r = 2$ we recover the usual formula for binomial numbers

$$\binom{m}{m_1, m_2} = \frac{m!}{m_1!m_2!} = \binom{m}{m_1} = \binom{m}{m-m_1} = \binom{m}{m_2}.$$

Indeed, to place m balls in two bins such that the first contains m_1 balls and the other $m_2 = m - m_1$ balls, it is enough to choose which balls go into the first bin, or which ones go into the second bin.

Analogous to the binomial theorem, we have the multinomial theorem.

Theorem 1.14.

$$(x_1 + x_2 + \cdots + x_r)^m = \sum_{\substack{m_1, m_2, \dots, m_r \\ \sum m_i = m, m_i \geq 0}} \binom{m}{m_1, m_2, \dots, m_r} x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}$$

Proof. The proof follows the same idea as the proof of the binomial theorem and it is left as an exercise. \square

Observe that setting $x_i = 1$ for all i in the binomial theorem we recover the fact that the total number of ways of placing m balls in r bins, regardless of the number of balls in each bin, is r^m .

1.5 Mappings

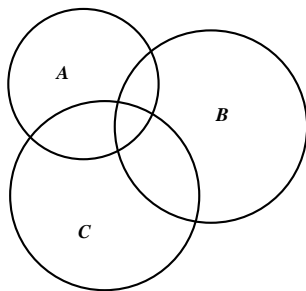
Many of the results in this section can be phrased in terms of maps. Let $\mathcal{F}(n, m)$ be the set of all mappings from $[n]$ to $[m]$. The following counting results are simple applications of the principles of this section.

- $|\mathcal{F}(n, m)| = m^n$
- For $n \leq m$, $\mathcal{F}(n, m)$ contains $m!/(m-n)!$ injective maps.
- There are $\binom{n}{k}$ maps in $\mathcal{F}(n, 2)$ such that the preimage of 1 is a set of size k .
- The number of maps $f \in \mathcal{F}(n, m)$ such that $f(1) < f(2) < \dots < f(n)$ is $\binom{m}{n}$.

2 The Principle of Inclusion and Exclusion

The Principle of Inclusion and Exclusion (PIE) is a very useful tool to count sets that can be expressed as a union or an intersection of simpler sets. The idea is to generalize the well-known formula to compute the cardinality of a union: $|A \cup B| = |A| + |B| - |A \cap B|$.

For the case of three sets it is also easy to find a formula by inspection:



$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

As we see, to compute the size of the union we sum the sizes of the components, subtract the intersections of pairs, and sum back the size of the triple intersection. The Principle of Inclusion and Exclusion is a generalization of this idea.

Theorem 2.1. (PIE) Let A_1, A_2, \dots, A_n be subsets of a set X . Then

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|. \end{aligned}$$

Proof. There are several proofs of the PIE. We choose one that has a more combinatorial flavour (as an exercise, prove it by induction). We check that the formula counts each element in $A_1 \cup A_2 \cup \dots \cup A_n$ just once. Let x be in $A_1 \cup A_2 \cup \dots \cup A_n$; by relabelling the sets if necessary, we can assume that x belongs to A_1, A_2, \dots, A_p but does not belong to A_{p+1}, \dots, A_n . Then in the RHS of the above formula, x contributes with

$$p - \binom{p}{2} + \binom{p}{3} - \dots + (-1)^{p-1} \binom{p}{p}.$$

This equals

$$\sum_{i=1}^p (-1)^{i-1} \binom{p}{i} = \sum_{i=0}^p (-1)^{i-1} \binom{p}{i} + 1 = 0 + 1 = 1,$$

since we know that the sum of signed binomials is zero. \square

Before looking at the applications, let us start with some remarks. The PIE is stated in terms of unions, but can also be used to count intersections. Indeed,

$$|A_1 \cap A_2 \cap \dots \cap A_n| = |(A_1^c \cup A_2^c \cup \dots \cup A_n^c)^c| = |X| - |A_1^c \cup A_2^c \cup \dots \cup A_n^c|,$$

where B^c stands for the complement of the set B in X . Now, using PIE,

$$|A_1 \cap \dots \cap A_n| = |X| - \sum_{i=1}^n |A_i^c| + \sum_{1 \leq i < j \leq n} |A_i^c \cap A_j^c| - \dots + (-1)^n |A_1^c \cap \dots \cap A_n^c|.$$

One of the main tricks in using PIE is to choose the sets A_i suitably so that computing the intersections $|A_{i_1} \cap \dots \cap A_{i_k}|$ is feasible. It is often the case that $|A_{i_1} \cap \dots \cap A_{i_k}|$ does not depend on the A_{i_j} but only on k , the number of sets in the intersection. In this case the PIE has a simpler form. Let A^k denote the size of the intersection of any k of the A_i . Then,

$$|A_1 \cup A_2 \cup \dots \cup A_n| = nA^1 - \binom{n}{2}A^2 + \binom{n}{3}A^3 - \dots + (-1)^{n-1}A^n.$$

The rest of this section is devoted to examples of application of the PIE.

Example. One of the classic applications of the Principle of Inclusion and Exclusion is the derangement problem.

Suppose n people leave their coats at the cloakroom of a theater. At the end of the play, the attendant gives the coats back without looking at the tickets. Which is the probability that nobody gets their own coat?

Let us identify the coats with the integers from 1 to n . Each way of giving back the coats is a permutation of $[n]$. For instance, the permutation $123 \dots n$ represents the case that each person gets back their own coat. Let π be a permutation of $[n]$. If for all i we have

$\pi(i) \neq i$, then nobody gets their own coat back. We call such permutations *derangements*. Then the probability asked is

$$\frac{\text{number of derangements of } [n]}{n!}.$$

Hence our goal is to compute the number of derangements of $[n]$; we denote the set of derangements by \mathcal{D}_n and its cardinality by d_n .

Let S_n be the set of the $n!$ permutations of n elements and for each i with $1 \leq i \leq n$ let A_i be the subset of all permutations π such that $\pi(i) = i$. By the remarks above, we have that

$$\mathcal{D}_n = A_1^c \cap A_2^c \cap \cdots \cap A_n^c = S_n - (A_1 \cup A_2 \cup \cdots \cup A_n).$$

Hence,

$$d_n = n! - |A_1 \cup A_2 \cup \cdots \cup A_n|,$$

and by PIE

$$d_n = n! - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

The only thing left now is to count the sizes of the intersections.

- $|A_i| = |\{\pi \in S_n | \pi(i) = i\}| = (n-1)!$, since the element i is fixed and we can permute the remaining $n-1$ in any way. Note that this is independent of the element i .
- $|A_i \cap A_j| = |\{\pi \in S_n | \pi(i) = i, \pi(j) = j\}| = (n-2)!$, since two elements are fixed and the remaining $n-2$ can be permuted arbitrarily. Again, the result is the same for all pairs i, j .

And in general,

- $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = (n-k)!$, for $1 \leq i_1 < i_2 < \cdots < i_k \leq n$.

Therefore,

$$d_n = n! - \sum_{i=1}^n (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^n \frac{(-1)^i}{i!}.$$

Hence, the probability asked is $\sum_{i=0}^n \frac{(-1)^i}{i!}$. Does this probability have a limit as n tends to infinite? Recall the series expansion for the exponential function $e^x = \sum_{i \geq 0} \frac{x^i}{i!}$; this series converges for all real values of x . Hence, as $n \rightarrow \infty$, the probability that nobody gets their own coat gets closer to $e^{-1} \sim 0.37$; actually, the rate of convergence is really fast, since the absolute error is bounded by $1/(n+1)!$.

Example. Euler's ϕ function.

Recall from elementary number theory the definition of the function ϕ of Euler. Given a positive integer n , $\phi(n)$ is the number of integers smaller than n that are relatively prime to n (including 1). For instance,

$$\phi(2) = |\{1\}| = 1, \quad \phi(3) = |\{1, 2\}| = 2, \quad \phi(4) = |\{1, 3\}| = 2, \quad \phi(5) = |\{1, 2, 3, 4\}| = 4.$$

Note that if n is prime, then $\phi(n) = n - 1$, since all integers smaller than n are relatively prime to n . Our goal is to find a formula for $\phi(n)$ for any integer n . We assume that we have the decomposition of n into prime factors,

$$n = \prod_{i=1}^r p_i^{\alpha_i},$$

where r is the number of distinct prime factors of n , the p_i are the distinct prime factors, and α_i stands for their multiplicities.

The integers that are relatively prime with n are those that do not contain any of the p_i as a factor. This suggests to define $B_i = \{m : m < n, p_i | m\}$, that is, the set of integers smaller than n that are divisible by p_i . Hence,

$$\phi(n) = |B_1^c \cap B_2^c \cap \cdots \cap B_r^c|.$$

By PIE,

$$\phi(n) = n - \sum_{i=1}^r |B_i| + \sum_{1 \leq i < j \leq r} |B_i \cap B_j| - \sum_{1 \leq i < j < k \leq r} |B_i \cap B_j \cap B_k| + \cdots + (-1)^r |B_1 \cap \cdots \cap B_r|.$$

Again, the problem reduces to computing the intersections of B_i 's. It is not difficult to show that

$$|B_{i_1} \cap \cdots \cap B_{i_k}| = |\{m : m < n, p_{i_1} \cdots p_{i_k} | m\}| = \frac{n}{p_{i_1} \cdots p_{i_k}}.$$

Note that in this case the size of $B_{i_1} \cap \cdots \cap B_{i_k}$ not only depends on k but also on the specific sets we intersect. Putting this into the formula given by PIE, we have

$$\phi(n) = n - n \left(\sum_{1 \leq i \leq r} \frac{1}{p_i} \right) + n \left(\sum_{1 \leq i < j \leq r} \frac{1}{p_i p_j} \right) + \cdots + (-1)^r n \frac{1}{p_1 \cdots p_r},$$

which can be written more compactly as

$$\phi(n) = n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \cdots \left(1 - \frac{1}{p_r} \right).$$

Example. The following is left as an exercise.

Show that the number of surjective maps from $[n]$ onto $[k]$ is

$$k^n - \binom{k}{1}(k-1)^n + \binom{k}{2}(k-2)^n + \cdots + (-1)^{k-1} \binom{k}{k-1} = \sum_{j=1}^k (-1)^{k-j} \binom{k}{j} j^n.$$

3 Integer and set partitions; Stirling numbers

3.1 Integer partitions

We introduced compositions as *ordered* sums, hence regarding $2 + 1$ and $1 + 2$ as different compositions of 3. But as partitions, we consider them the same.

Definition 3.1. A partition of an integer n is an expression of n as a sum of positive integers

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k \quad \text{with} \quad \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1.$$

We usually denote this partition by $(\lambda_1, \lambda_2, \dots, \lambda_k)$.

Example. Let us look at the partitions of the first integers.

$$\begin{aligned} 1 \\ 2 &= 1 + 1 \\ 3 &= 2 + 1 = 1 + 1 + 1 \\ 4 &= 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1 \\ 5 &= 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 \end{aligned}$$

We denote by $p(n)$ the number of partitions of the integer n and by $p_k(n)$ the number of partitions of n with k parts. From the example above we have $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$. There are no explicit formulas known for $p(n)$ ¹. But nevertheless integer partitions are one of the nicest² and richest objects in combinatorics.

We start with a recursion for the numbers $p_k(n)$.

Proposition 3.2. For $n \geq k \geq 2$,

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k).$$

Proof. Let λ be a partition of n with k parts. We compute $p_k(n)$ by counting partitions according to whether the last part λ_k is 1 or greater than 1.

- There are as many partitions of n with k parts and $\lambda_k = 1$ as partitions of $n-1$ with $k-1$ parts.
- If $\lambda_k > 1$, then all parts are greater than 1, hence we can subtract 1 from each part and get a partition of $n-k$ with k parts.

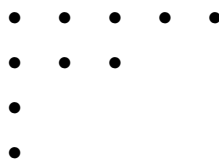
□

This recurrence and the trivial cases $p_1(n) = 1$ and $p_0(0) = 1$ allow us to compute the numbers $p_k(n)$ (Table 2), in the same spirit as Pascal's triangle.

n	$p(n)$	$p_1(n)$	$p_2(n)$	$p_3(n)$	$p_4(n)$	$p_5(n)$	$p_6(n)$	$p_7(n)$	$p_8(n)$
1	1	1							
2	2	1	1						
3	3	1	1	1					
4	5	1	2	1	1				
5	7	1	2	2	1	1			
6	11	1	3	3	2	1	1		
7	15	1	3	4	3	2	1	1	
8	22	1	4	5	5	3	2	1	1

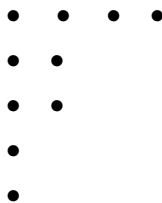
Table 2: Integer partitions according to the number of parts.

A very useful way to represent partitions is by the means of *Ferrers diagrams*. For a partition $(\lambda_1, \lambda_2, \dots, \lambda_k)$, its Ferrers diagram is constructed by placing, left justified and from top to bottom³, λ_1 dots, λ_2 dots, \dots , λ_k dots. This is better understood with an example. The Ferrers diagram for the partition $5 + 3 + 1 + 1$ is



As an exercise, interpret Proposition 3.2 above in terms of Ferrers diagrams.

Given a partition λ , its *conjugate* μ is the partition whose Ferrers diagram is obtained by reflecting the Ferrers diagram of λ along the diagonal $y = -x$. That is, instead of reading the diagram by rows, we read it by columns. For instance, the conjugate of $(5, 3, 1, 1)$ is $(4, 2, 2, 1, 1)$.



The following description of the conjugate of a partition follows easily by looking at the Ferrers diagram.

¹The asymptotic behaviour is known. If this sounds interesting, you may look at Thm. 15.7 of Van Lint and Wilson, *A course in combinatorics*, Cambridge UP. You may want to wait until we have studied generating functions though.

²Well, this is a personal opinion.

³This is the English notation. In French notation, Ferrers diagrams are drawn with the largest part at the bottom.

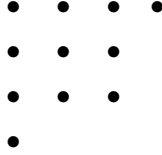
Proposition 3.3. *If λ is a partition of n , then its conjugate μ is also a partition of n and*

$$\mu_j = |\{i | \lambda_i \geq j\}|.$$

The following result also follows by reasoning on Ferrers diagrams and conjugate partitions.

Proposition 3.4. *The number of partitions of n with k parts equals the number of partitions of n whose largest part is k .*

A partition is called *self-conjugate* if it equals its conjugate; or, equivalently, if the Ferrers diagram is symmetric with respect to its diagonal. For instance, $(4, 3, 3, 1)$ is a self-conjugate partition.



Proposition 3.5. *The number of self-conjugate partitions of n equals the number of partitions of n all whose parts are odd and distinct.*

Proof. We give a proof *by picture*. We define a bijection between self-conjugate partitions and partitions whose parts are odd and distinct, see Figure 1.

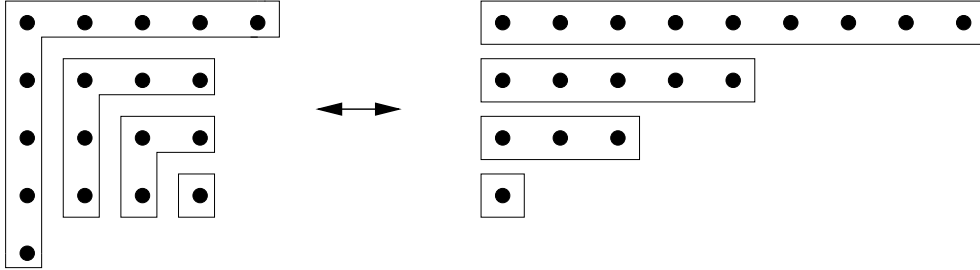


Figure 1: Bijection between self-conjugate partitions and partitions all whose parts are odd and different.

This bijection can be defined formally in the following way. Let $(\lambda_1, \dots, \lambda_t)$ be a self-conjugate partition. Consider the partition given by $\mu_i = 2(\lambda_i - (i - 1)) - 1$ for i such that $\lambda_i > i - 1$. Check that all parts of μ are odd and different.

Conversely, given a partition (μ_1, \dots, μ_s) with all parts odd and different, define $\lambda_j = (\mu_j + 1)/2 + (j - 1)$ for $1 \leq j \leq s$. For $k \geq s + 1$, let $\lambda_j = |\{\lambda_i : i \leq s, \mu_i \geq j\}|$ (as long as this is non-zero). The partition λ is self-conjugate.

□

For the moment, we finish our discussion about partitions with a quite surprising result. We delay its proof until we develop some generating function tools later in the course. But of course you are allowed (and encouraged) to think about a combinatorial proof⁴.

Theorem 3.6. *The number of partitions of n into odd parts is the same as the number of partitions of n into different parts.*

3.2 Set partitions

One of the first questions we studied was choosing a k -subset of an n -set. Observe that picking a subset A of a set X is the same as partitioning X into two disjoint subsets, A and A^c . So we can ask the question: in how many ways can we partition an n -set X into two disjoint non-empty subsets? (By a *partition* of X into two subsets we mean picking A and B such that $A \cap B = \emptyset$ and $X = A \cup B$.) The answer is quite simple. We have $2^n - 2$ choices for the first subset, say A (\emptyset and X are not valid choices), and once A is determined, we have that $B = A^c$. Observe though that the order of A and B is irrelevant, hence we have to divide by 2 and the result is $(2^n - 2)/2 = 2^{n-1} - 1$. We now generalize these ideas to partitions of sets into k blocks.

Definition 3.7. *A partition of a set X is a decomposition of X of the form $X = A_1 \cup \dots \cup A_k$ with $A_i \neq \emptyset$ for all i and $A_i \cap A_j = \emptyset$ for all $i \neq j$. The sets A_i are called the blocks of the partition. Note that partitions are defined regardless of the order of the blocks.*

Example. Let us list all possible partitions of the sets $[1]$, $[2]$ and $[3]$.

$$[1] = \{1\}$$

$$[2] = \{1, 2\} = \{1\} \cup \{2\}$$

$$[3] = \{1, 2, 3\} = \{1, 2\} \cup \{3\} = \{1, 3\} \cup \{2\} = \{1\} \cup \{2, 3\} = \{1\} \cup \{2\} \cup \{3\}$$

The number of partitions of an n -set into k blocks is denoted by $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ and it is called a *Stirling number of the second kind*⁵. (An alternative notation, though less common nowadays, is $S(n, k)$.) The total number of partitions of an n -set is denoted by $B(n)$ and it is called a *Bell number*. By definition, $B(n) = \sum_{k=1}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$.

Example. The following values of Stirling and Bell numbers are easily deduced or computed ($n \geq 1$).

$$\left\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right\} = 1 \quad \left\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \right\} = 0 \quad \left\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right\} = 1 \quad \left\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \right\} = 2^{n-1} - 1 \quad \left\{ \begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right\} = \binom{n}{2} \quad \left\{ \begin{smallmatrix} n \\ n \end{smallmatrix} \right\} = 1$$

$$B(1) = 1 \quad B(2) = 2 \quad B(3) = 5 \quad B(4) = 15$$

Like the number of integer partitions, Stirling numbers of the second kind satisfy a linear recurrence that allows an easy recursive computation.

⁴Or cheat by reading Section 3.3 of Stanton and White, *Constructive Combinatorics*, Springer, 1986.

⁵The first kind will appear soon.

n	$\left\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right\}$	$\left\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \right\}$	$\left\{ \begin{smallmatrix} n \\ 3 \end{smallmatrix} \right\}$	$\left\{ \begin{smallmatrix} n \\ 4 \end{smallmatrix} \right\}$	$\left\{ \begin{smallmatrix} n \\ 5 \end{smallmatrix} \right\}$	$\left\{ \begin{smallmatrix} n \\ 6 \end{smallmatrix} \right\}$	$B(n)$
1	1						1
2	1	1					2
3	1	3	1				5
4	1	7	6	1			15
5	1	15	25	10	1		52
6	1	31	90	65	15	1	203

Table 3: Stirling numbers of the second kind and Bell numbers.

Proposition 3.8. For $n \geq k \geq 1$,

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\} + k \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\}.$$

Proof. We count partitions of $[n]$ according to whether $\{n\}$ is a block or not.

- If $\{n\}$ is a block of the partition, the remaining $n-1$ elements have to be partitioned into $k-1$ blocks, hence there are $\left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\}$ choices.
- If $\{n\}$ is not a block, the element n is in one of the k blocks together with some other elements. Partition first the set $[n-1]$ into k blocks, and then choose any of the k blocks and adjoin n to it. We have $\left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\}$ choices for the partition, and k choices for the block that contains n .

□

This recurrence can be used to compute some values of Stirling and Bell numbers (Table 3).

Bell numbers can also be computed recursively, although in this case the recurrence involves all previous terms.

Proposition 3.9.

$$B(n+1) = \sum_{k=0}^n \binom{n}{k} B(k)$$

Proof. We count partitions of $[n+1]$ according to the size of the block that contains $n+1$. Say that the block containing $n+1$ has size j , for some j with $1 \leq j \leq n+1$. There are $\binom{n}{j-1}$ choices for the other elements of the block, and once this is chosen, the remaining $n+1-j$ elements have to be partitioned, which can be done in $B(n+1-j)$ ways. Therefore,

$$B(n+1) = \sum_{j=1}^{n+1} \binom{n}{j-1} B(n+1-j) = \sum_{j=1}^{n+1} \binom{n}{n-j+1} B(n+1-j) = \sum_{k=0}^n \binom{n}{k} B(k).$$

□

There is actually an explicit formula for Stirling numbers of the second kind based in a correspondance between set partitions and surjective mappings. Let f be a surjective map from $[n]$ to $[k]$. The sets $f^{-1}(1), f^{-1}(2), \dots, f^{-1}(k)$ form a partition of $[n]$ (since f is surjective, none of these sets is empty). Observe that this correspondance gives each partition into k blocks a total of $k!$ times, since switching the preimages gives the same partition but a different map. Hence, $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is the number of surjective maps from $[n]$ to $[k]$, which we already know. Therefore,

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \frac{1}{k!} \sum_{j=1}^k (-1)^{k-j} \binom{k}{j} j^n.$$

3.3 Decomposition of permutations into disjoint cycles

Finally, we briefly discuss the decomposition of permutations into disjoint cycles and Stirling numbers of the first kind.

Usually we write a permutation π of $[n]$ as an ordered sequence $a_1 a_2 \dots a_n$ of the numbers $\{1, 2, \dots, n\}$. A permutation can be viewed as a bijection from $[n]$ onto itself, defined by $\pi(i) = a_i$. For instance, 23541 denotes the permutation $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 5, 4 \rightarrow 4, 5 \rightarrow 1$. Another way of writing permutations is the *disjoint cycle* notation⁶. The permutation above in disjoint cycle notation is (1235)(4). Each permutation can be written uniquely as a product of disjoint cycles up to the order of the cycles and the cyclic order of the elements in each cycle (a cycle of length k can be written in k ways).

We associate with each permutation π of \mathcal{S}_n an n -tuple (c_1, c_2, \dots, c_n) , where c_i is the number of cycles of length i in the disjoint cycle decomposition of π . This n -tuple is called the *type* of the permutation. The permutation of our example has type $(1, 0, 0, 1, 0)$.

Proposition 3.10. *The number of permutations of type (c_1, c_2, \dots, c_n) is*

$$\frac{n!}{c_1! \dots c_n! 1^{c_1} 2^{c_2} \dots n^{c_n}}$$

Proof. Let $\pi = x_1 x_2 \dots x_n$ be any permutation of $[n]$. Parenthesize the word π so that the first c_1 cycles have length 1, the next c_2 have length 2, and so on. The result is the disjoint cycle notation of a permutation of cycle type (c_1, c_2, \dots, c_n) . But this procedure gives the same permutation several times. Let us count how many times a permutation of cycle type (c_1, c_2, \dots, c_n) will appear. First, each cycle of length c can be written in c different ways; so just taking into account this, each permutation is repeated $1^{c_1} 2^{c_2} \dots n^{c_n}$ times. But the relative order of the cycles of the same length is irrelevant, ie, the c_1 cycles of length 1 can be ordered in $c_1!$ ways, the c_2 cycles of length 2 in $c_2!$ ways, etc... Hence, each permutation is counted $c_1! c_2! \dots c_n! 1^{c_1} 2^{c_2} \dots n^{c_n}$ times, hence the formula. \square

If instead of the type of a permutation we are only interested in the number of cycles in its decomposition, we obtain Stirling numbers of the first kind.

⁶See any basic group theory book if you are not familiar with this.

Definition 3.11. *The number of permutations of $[n]$ whose cycle decomposition contains k cycles is denoted by $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ and is called a Stirling number of the first kind. (In old notation, $s(n, k)$.)*

Clearly $\left[\begin{smallmatrix} n \\ n \end{smallmatrix} \right] = 1$, since the only permutation in S_n that decomposes as n cycles is the identity (all cycles must have length one). The number $\left[\begin{smallmatrix} n \\ 1 \end{smallmatrix} \right]$ counts permutations that decompose as a unique cycle, hence permutations that are cycles; their cycle type is $(0, \dots, 0, 1)$, and by the previous result there are $(n-1)!$ of them. It is also easy to determine $\left[\begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right]$; if we have $n-1$ cycles, the cycle type must be $(n-2, 1, 0, \dots, 0)$, hence $\left[\begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right] = \frac{n!}{2!(n-2)!} = \binom{n}{2}$. The sum over k of the Stirling numbers $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ should be the total number of permutations of an n -element set, which we know is $n!$.

Like Stirling numbers of the second kind, the numbers $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ also satisfy a recurrence.

Proposition 3.12. *For $n \geq k \geq 1$,*

$$\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right] + (n-1) \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right].$$

Proof. We count permutations according to whether n is a fix point or not (ie, according to whether (n) is a cycle of the decomposition).

- If (n) is a cycle, the remaining $n-1$ integers give a permutation with $k-1$ cycles, so this gives the term $\left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right]$.
- If (n) is not a cycle, then the element n is in a cycle of length at least 2. Take a permutation $\pi \in S_{n-1}$ with k cycles; then we can insert the element n after any of the numbers $1, 2, \dots, n-1$ in the disjoint cycle decomposition of π . This yields a permutation in S_n in which n is not a fix point. So there are $\left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right]$ choices for the permutation and $n-1$ choices for the position in which to insert n .

□

We can now use this recurrence to generate a table of Stirling numbers of the first kind (Table 4).

4 Generating functions and recurrences

Up to this point, our answers to enumerative problems have consisted only of closed formulas, such as $c(n) = 2^{n-1}$. But as we have seen in the case of partitions, these closed formulas are not always easy to find, if known. We have also studied some problems by means of recurrences, that do not provide closed formulas but allow us to compute as many terms as we like. These and the following sections deal with another way of expressing the result of a counting problem, namely generating functions. With them we shall be able to give more information about old and new counting sequences, and solve a variety of problems that were out of reach with the basic techniques of the previous chapters.

n	$\begin{bmatrix} n \\ 1 \end{bmatrix}$	$\begin{bmatrix} n \\ 2 \end{bmatrix}$	$\begin{bmatrix} n \\ 3 \end{bmatrix}$	$\begin{bmatrix} n \\ 4 \end{bmatrix}$	$\begin{bmatrix} n \\ 5 \end{bmatrix}$	$\begin{bmatrix} n \\ 6 \end{bmatrix}$
1	1					
2	1	1				
3	2	3	1			
4	6	11	6	1		
5	24	50	35	10	1	
6	120	274	225	85	15	1

Table 4: Stirling numbers of the first kind.

Let us start by formalizing our goals. Given a problem, the answer we look for is a sequence of numbers a_0, a_1, a_2, \dots , such as 1, 1, 2, 3, 5, 7, 11, 15, \dots if we are counting integer partitions. To this sequence we associate a generating function.

Definition 4.1. The (ordinary)⁷ generating function (OGF) of a sequence $\{a_n\}_{n \geq 0}$ is the formal power series

$$a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \dots = \sum_{n \geq 0} a_n z^n.$$

By a “formal power series” we mean that the variable z does not take any value and we regard it just as a “mark” (we will formalize this soon). We do not care about convergence issues either. So in principle it does not seem that a generating function is going to be more useful than a recurrence...

Example. Fix some integer m . The sequence $\{\binom{m}{k}\}_{k \geq 0}$ has as generating function

$$\sum_{k \geq 0} \binom{m}{k} z^k = \binom{m}{0} + \binom{m}{1} z + \binom{m}{2} z^2 + \dots + \binom{m}{m} z^m = (1 + z)^m.$$

So in this case, the generating function is not an infinite series but a polynomial.

Example. Consider the sequence 1, 1, 1, 1, \dots . Although it does not seem combinatorially attractive, this sequence and its generating function will be of extreme importance to us. The generating function is

$$F(z) = 1 + z + z^2 + z^3 + \dots$$

Observe that $F(z) - zF(z) = 1$, hence $F(z) = \frac{1}{1-z}$. This is the well-known formula for the sum of a geometric series; as mentioned before, in this context we do not care about analytic or convergence properties of $F(z)$. By making the substitution $z \rightarrow az$, one shows that the generating function for the sequence $1, a, a^2, a^3, \dots$ is $\frac{1}{1-az}$.

We will soon justify that the preceding operations on formal power series are well defined and sound, but before doing so we examine other examples and start exploring the spirit of “generatingfunctionology”, as it is sometimes called⁸.

⁷The other class of generating functions that we will study in this course are exponential generating functions.

⁸Herbert S. Wilf, *Generatingfunctionology*, Academic Press, 1990.

Let $a(z)$ be the OGF of the sequence $\{a_n\}_{n \geq 0}$, that is $a(z) = \sum_{n \geq 0} a_n z^n$. We might want to express in terms of $a(z)$ some slight variations of this series, such as $\sum_{n \geq 0} a_{n-1} z^n$ or $\sum_{n \geq 0} n a_n z^n$. After some thought, the following table is derived (Table 5).

series	closed form for OGF
$\sum_{n \geq 0} a_n z^n$	$a(z)$
$\sum_{n \geq 1} a_{n-1} z^n$	$z a(z)$
$\sum_{n \geq 0} a_{n+1} z^n$	$\frac{a(z) - a_0}{z}$
$\sum_{n \geq 0} a_{n+k} z^n$	$\frac{a(z) - a_0 - a_1 z - \dots - a_{k-1} z^{k-1}}{z^k}$
$\sum_{n \geq 0} b_n z^n$	$b(z)$
$\sum_{n \geq 0} (a_n + b_n) z^n$	$a(z) + b(z)$

Table 5: Operations on OGF's.

These rules can now be used to find the OGF of a sequence given by a recurrence relation. For instance, consider the sequence defined by

$$a_0 = 1, \quad a_1 = 1, \quad a_{n+2} = a_{n+1} + a_n \quad \text{for } n \geq 0$$

Multiply both sides of the recurrence by z^n :

$$a_{n+2} z^n = a_{n+1} z^n + a_n z^n$$

and sum over all $n \geq 0$:

$$\sum_{n \geq 0} a_{n+2} z^n = \sum_{n \geq 0} a_{n+1} z^n + \sum_{n \geq 0} a_n z^n.$$

By using the rules in the previous table, we get

$$\frac{a(z) - 1 - z}{z^2} = \frac{a(z) - 1}{z} + a(z).$$

Solving this equation for $a(z)$ we deduce

$$a(z) = \frac{1}{1 - z - z^2}.$$

How can this generating function help us understand better the sequence given by the recurrence relation?

Ideally, we would like to find a closed formula for the numbers a_n . In some situations, like the present one, this is possible. First of all, we expand $\frac{1}{1-z-z^2}$ in partial fractions.

We first decompose the denominator in linear factors:

$$1 - z - z^2 = (1 - \alpha z)(1 - \beta z).$$

Equating the coefficients of the powers of z one finds

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

(α and β are the inverses of the roots of $1 - z - z^2$.) Now we find constants A and B such that

$$\frac{1}{1 - z - z^2} = \frac{A}{1 - \alpha z} + \frac{B}{1 - \beta z} = \frac{A + B - (\alpha A + \beta B)z}{(1 - \alpha z)(1 - \beta z)}.$$

By equating the powers of z we obtain the system of equations

$$\begin{cases} A + B = 1; \\ \alpha A + \beta B = 0. \end{cases}$$

whose solution is $A = \frac{\alpha}{\alpha - \beta}$, $B = \frac{-\beta}{\alpha - \beta}$. Hence,

$$a(z) = \frac{1}{1 - z - z^2} = \frac{1}{\sqrt{5}} \left(\frac{\alpha}{1 - \alpha z} - \frac{\beta}{1 - \beta z} \right)$$

Now recall that $\frac{1}{1 - az} = \sum_{n \geq 0} a^n z^n$. Hence,

$$a(z) = \frac{1}{\sqrt{5}} \left(\sum_{n \geq 0} \alpha^{n+1} z^n - \sum_{n \geq 0} \beta^{n+1} z^n \right).$$

By definition of a generating function, a_n is the coefficient of z^n in $a(z)$. Therefore, we have that

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

By finding their generating function first, we have been able to find a formula for the numbers a_n . These numbers a_n are called the *Fibonacci numbers*⁹. Imagine now that we are not that interested in an exact formula for a_n , but rather we want to know approximately how fast Fibonacci numbers grow. Note that for large values of n , the term $-(\frac{1-\sqrt{5}}{2})^{n+1}$ can be neglected, and actually will never be as large as 0.5. Hence,

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

Even for small n this approximation is extremely good (it will always be at most 0.5 off the true value; actually, since we know that a_n is an integer, we conclude that a_n is the integer nearest to the approximate value). By using MAPLE¹⁰ we obtain the following numerical results.

⁹Most combinatorics textbooks contain the problem of rabbit breeding that originally lead to Fibonacci numbers.

¹⁰Or another computer algebra package.

a_n	1	1	2	3	5	8	13	21
$a_n \sim$	0.72...	1.17...	1.89...	3.06...	4.95...	8.02...	12.98...	21.00...
...	34	55	89	144				
	33.99...	55.00...	88.99...	144.00...				

In other situations we will not be as lucky and a closed formula for the coefficients will not be available. In those cases, there is still much that can be said, especially in terms of asymptotic approximations. Unfortunately, this issue goes further beyond the scope of this course¹¹.

4.1 Formal power series

The purpose of this section is to develop the theory of formal power series to provide a valid framework in which to carry out our computations with generating functions.

Definition 4.2. A formal power series is an expression of the form $a_0 + a_1z + a_2z^2 + a_3z^3 + \dots$, where $a_0, a_1, a_2, a_3, \dots$ are rational numbers¹². The set of all power series is denoted by $\mathbb{Q}[[z]]$.

Again, the variable z has to be interpreted as a “mark”. Observe that not all terms need to be different from zero. For instance 4 , $1+z$, and z^{13} are formal power series. If $f(z)$ is a formal power series, we denote by $[z^n]f(z)$ the coefficient of z^n in $f(z)$. For example, $[z](1+z) = 1$, $[z^0](4+z^4) = 4$, and $[z](1+z^2) = 0$. If a formal power series is called $a(z)$, we use the same letter for the coefficients: a_0, a_1, a_2, \dots .

We can define operations on formal power series as one would expect. Their sum is defined as

$$a(z) + b(z) = \sum_{n \geq 0} (a_n + b_n) z^n.$$

The product is a bit trickier but also natural:

$$a(z)b(z) = \sum_{n \geq 0} \left(\sum_{0 \leq i \leq n} a_i b_{n-i} \right) z^n.$$

Observe that $(1-z)(1+z+z^2+\dots) = 1$. Hence it makes sense to write

$$\frac{1}{1-z} = 1 + z + z^2 + \dots$$

Definition 4.3. We say that $b(z)$ is the (multiplicative) inverse of $a(z)$ if $a(z)b(z) = 1$.

Proposition 4.4. The formal power series $a(z)$ has a multiplicative inverse if and only if $a_0 \neq 0$.

¹¹The interested reader will find countless examples in Flajolet and Sedgewick’s forthcoming book *Analytic combinatorics*, especially in the parts devoted to complex asymptotics. The preliminary version of the book is available on-line at <http://algo.inria.fr/flajolet/Publications/books.html>.

¹²Actually, any other field as the real or complex numbers would do.

Proof. Suppose first that $a(z)$ has an inverse. Then there exists a formal power series $b(z)$ such that

$$(a_0 + a_1z + a_2z^2 + \cdots)(b_0 + b_1z + b_2z^2 + \cdots) = 1.$$

By the definition of product of power series, we deduce that $a_0b_0 = 1$, hence that $a_0 \neq 0$.

Conversely, suppose now that $a_0 \neq 0$ and consider the equation

$$(a_0 + a_1z + a_2z^2 + \cdots)(b_0 + b_1z + b_2z^2 + \cdots) = 1.$$

We show that this equation can be solved for the b_n 's, and hence that $a(z)$ has an inverse. Expand the product and equate coefficients of z in both sides:

$$a_0b_0 = 1 \Rightarrow b_0 = \frac{1}{a_0},$$

since $a_0 \neq 0$. Also,

$$a_0b_1 + a_1b_0 = 0 \Rightarrow b_1 = \frac{-a_1}{a_0^2},$$

$$a_0b_2 + a_1b_1 + a_2b_0 = 0 \Rightarrow b_2 = \frac{-a_2a_0 - a_1^2}{a_0^3},$$

and similarly we can inductively find b_3, b_4, \dots . Hence $a(z)$ has a multiplicative inverse. \square

At this point we have endowed the set $\mathbb{Q}[[z]]$ with a sum and a product; it is easy to check that these two operations are associative and commutative, and that the sum is distributive with respect to the product. Hence $\mathbb{Q}[[z]]$ is a commutative ring with unity.

The following is the binomial theorem for negative integer exponents.

Proposition 4.5. *As formal power series, for integer $k \geq 0$*

$$\frac{1}{(1-z)^k} = \sum_{n \geq 0} \binom{n+k-1}{n} z^n$$

Proof.

$$\frac{1}{(1-z)^k} = (1 + z + z^2 + z^3 + \cdots)^k$$

The coefficient of z^n above equals the number of ways of picking one power of z from each of the k factors, such that the sum of the exponents is n . In other words, the coefficient of z^n is the number of solutions to the equation $e_1 + e_2 + \cdots + e_k = n$, with $e_i \geq 0$. But we know from Theorem 1.11 that this number is $\binom{n+k-1}{n}$. \square

Another operation on power series is composition. Given two power series $a(z)$ and $b(z)$, their *composition* is the series $a(b(z)) = \sum_{n \geq 0} a_n(b(z))^n$. But is this operation meaningful? Each term $a_n(b(z))^n$ is well defined, but taking an infinite sum could lead to some problems. Suppose that $b_0 \neq 0$. Then each term $b(z)^n$ contributes with a non-zero constant term b_0^n . Hence the constant term of $a(b(z))$ is $\sum_{n \geq 0} a_n b_0^n$, and this sum may easily be divergent. To

avoid this problem, we only consider composition of series with constant term equal to zero, or such that $a(z)$ is a polynomial. In this case, we have that

$$[z^n]a(b(z)) = \sum_{k=0}^n [z^n](a_k b(z)^k).$$

Example. Take $a(z) = 1/(1-z)$ and $b(z) = z^2$. Then $a(b(z)) = 1/(1-z^2) = 1 + z^2 + z^4 + z^6 + \dots$

The *formal derivative* of the power series $a(z) = \sum_{n \geq 0} a_n z^n$ is the power series $a'(z) = \sum_{n \geq 0} n a_n z^{n-1}$. This formal derivative satisfies the usual rules with respect to sums, products, quotients, composition, etc. . .

We use the familiar terminology from analysis to denote some power series. For instance, we denote $\sum_{n \geq 0} \frac{1}{n!} z^n$ by $\exp(z)$ and $\sum_{n \geq 1} \frac{1}{n} z^n$ by $\log(\frac{1}{1-z})$. In analysis we have the equality $\exp(\log(\frac{1}{1-z})) = \frac{1}{1-z}$. Is this equality true at the level of formal power series? Here is where we use some analysis. Observe that the series $\sum_{n \geq 0} \frac{1}{n} z^n$ converges for $|z| < 1$ and the exponential series converges for all z . Hence the composition $\exp(\log(\frac{1}{1-z}))$ converges for $|z| < 1$. But if it converges, it should converge to the true value, that is, $\frac{1}{1-z}$. So we deduce that the series $\exp(\log(\frac{1}{1-z}))$ and $\frac{1}{1-z}$ are the same in a neighbourhood of the origin. But if they are the same in a no matter how small neighbourhood of the origin, they have the same coefficients in their Taylor expansions, and hence they also agree as formal power series.

This same idea can be used to prove the generalized binomial theorem for rational exponents.

Proposition 4.6. For all $a \in \mathbb{Q}$,

$$(1+z)^a = \sum_{n \geq 0} \binom{a}{n} z^n,$$

where $\binom{a}{n} = \frac{a(a-1)(a-2)\dots(a-n+1)}{n!}$.

So the working rule to remember with power series is that, although the variable plays just a “mark” role and takes no value, things behave as our intuition from analysis suggests.

4.2 Linear recurrences

We have already seen several recurrences in this course. In this part we show how generating functions can help solving recurrences. Mostly we will do this by example. But let us first define recurrences formally.

Definition 4.7. A recurrence for a sequence $\{a_n\}_{n \geq 0}$ is a relation of the form

$$a_{n+k} = \phi(a_n, a_{n+1}, \dots, a_{n+k-1})$$

valid for all $n \geq 0$. The values a_0, a_1, \dots, a_{k-1} are the initial conditions of the recurrence, and k is the order or the recurrence.

For instance, the recurrence for the Fibonacci numbers has order 2.

Example. Find the number b_n of binary words that do not have two consecutive zeros.

Let us start by computing the first values of b_n . It is easy to check that $b_0 = 1$ (the empty word), $b_1 = 2$ (the words 0 and 1), and $b_2 = 3$ (01, 10, and 11). In order to find a recurrence for b_n , we have to somehow decompose a word with no two consecutive zeros into smaller words. Suppose that $w_1 w_2 \cdots w_n$ is a binary word with no two consecutive zeros. We distinguish two cases. On the one hand, if $w_n = 1$, then $w_1 w_2 \cdots w_{n-1}$ is also a binary word with no two consecutive zeros. On the other hand, if $w_n = 0$, then we must have $w_{n-1} = 1$, and hence $w_1 w_2 \cdots w_{n-2}$ is a binary word with no two consecutive zeros. Therefore,

$$b_n = b_{n-1} + b_{n-2} \quad \text{for } n \geq 2$$

or equivalently,

$$b_{n+2} = b_{n+1} + b_n \quad \text{for } n \geq 0.$$

Is this is the same recurrence as for Fibonacci numbers. Observe that a recurrence also includes the initial conditions, and in this case they are different ($b_0 = 1$, $b_1 = 2$). We solve the recurrence using the same method as for Fibonacci numbers. We multiply both sides by z^n and sum over all $n \geq 0$.

$$\sum_{n \geq 0} b_{n+2} z^n = \sum_{n \geq 0} b_{n+1} z^n + \sum_{n \geq 0} b_n z^n$$

Let $b(z)$ be the corresponding generating function. Applying the rules we deduce

$$\frac{b(z) - 1 - 2z}{z^2} = \frac{b(z) - 1}{z} + b(z),$$

and hence

$$b(z) = \frac{1 + z}{1 - z - z^2}.$$

Observe that the denominator is the same as we had for Fibonacci numbers, whereas the numerator is different. As we shall see, it is always the case in dealing with linear recurrences that the initial conditions determine the numerator and the recurrence determines the denominator. By using the technique of partial fractions, we get to an explicit formula for b_n , namely

$$b_n = \frac{1 + \alpha}{\alpha - \beta} \alpha^n - \frac{1 - \beta}{\alpha - \beta} \beta^n,$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Observe that the asymptotic behaviour is the same as for Fibonacci numbers. This is another general fact, that the recurrence determines the growth rate, regardless of the initial conditions.

A recurrence is *linear with constant coefficients* if it is of the form

$$a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n = 0$$

for some rational numbers c_1, c_2, \dots, c_k . Linear recurrences with constant coefficients have very special generating functions. The following is a basic theorem whose proof is left as an exercise (just mimic our procedure for solving recurrences).

Theorem 4.8. Let $\{a_n\}_{n \geq 0}$ be a sequence. The following are equivalent.

- $\{a_n\}_{n \geq 0}$ satisfies a linear recurrence with constant coefficients $a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \dots + c_k a_n = 0$.
- Its generating function $a(z)$ is of the form $\frac{P(z)}{1+c_1 z+c_2 z^2+\dots+c_k z^k}$, where $P(z)$ is a polynomial in z of degree at most $k-1$.

Generating functions that are of the form $\frac{P(z)}{Q(z)}$ for some polynomials $P(z), Q(z)$ are called *rational*¹³. They are the simplest kind of generating functions, and they arise from linear recurrences. If we have a sequence whose GF is rational, we can use the method of partial fractions to find an explicit formula for the terms of the recurrence. Let us sketch the procedure briefly.

We first decompose the denominator as $Q(z) = (1 - \alpha_1 z)^{d_1} (1 - \alpha_2 z)^{d_2} \dots (1 - \alpha_r z)^{d_r}$. That is, the α_i^{-1} are the roots of $Q(z)$ and the d_i are their multiplicities. By the theory of partial fractions, we know that there exist complex numbers $A_{i,j}$ for $1 \leq i \leq r$ and $1 \leq j \leq d_i$ such that

$$\frac{P(z)}{Q(z)} = \frac{A_{1,1}}{1 - \alpha_1 z} + \frac{A_{1,2}}{(1 - \alpha_1 z)^2} + \dots + \frac{A_{1,d_1}}{(1 - \alpha_1 z)^{d_1}} + \frac{A_{2,1}}{1 - \alpha_2 z} + \dots + \frac{A_{r,d_r}}{(1 - \alpha_r z)^{d_r}}$$

From this expression we want to extract the coefficient of z^n . Recall that

$$\frac{1}{(1 - \alpha z)^d} = \sum_{n \geq 0} \binom{n+d-1}{n} \alpha^n z^n.$$

Hence,

$$\begin{aligned} [z^n] \frac{P(z)}{Q(z)} &= \left(A_{1,1} + A_{1,2} \binom{n+2-1}{n} + \dots + A_{1,d_1} \binom{n+d_1-1}{n} \right) \alpha_1^n + \\ &\quad \left(A_{2,1} + \dots + A_{2,d_2} \binom{n+d_2-1}{n} \right) \alpha_2^n + \dots + \left(A_{r,1} + \dots + A_{r,d_r} \binom{n+d_r-1}{n} \right) \alpha_r^n \end{aligned}$$

So we have just proved one direction of the following theorem. The other direction follows easily by working backwards.

Theorem 4.9. If the sequence $\{a_n\}_{n \geq 0}$ has a rational generating function $\frac{P(z)}{Q(z)}$ with $\deg(P(z)) < \deg(Q(z))$, then

$$a_n = P_1(n) \alpha_1^n + P_2(n) \alpha_2^n + \dots + P_r(n) \alpha_r^n,$$

where $\alpha_1^{-1}, \dots, \alpha_r^{-1}$ are the roots of $Q(z)$ and each $P_i(n)$ is a polynomial of degree $d_i - 1$, where d_i is the multiplicity of the root α_i^{-1} . Conversely, every sequence with a general term of this form has a rational generating function.

¹³In general, we will assume that $\deg(P(z)) < \deg(Q(z))$; if this is not the case, divide $P(z)$ by $Q(z)$ and observe that by modifying a finite number of terms in our sequence we can assume that the generating function is $P'(z)/Q(z)$ with $\deg(P'(z)) < \deg(Q(z))$.

Let us see how Theorems 4.8 and 4.9 work. The advantage is that we do not have to carry out all the steps.

Example. Consider the recurrence $a_{n+3} = 4a_{n+2} - 5a_{n+1} + 2a_n$, with initial conditions $a_0 = 2, a_1 = 2, a_2 = 3$. Since this is a linear recurrence with constant coefficients, we know that its generating function is rational and it is of the form

$$\frac{P(z)}{1 - 4z + 5z^2 - 2z^3},$$

where $P(z)$ is a polynomial of degree at most 2. Now we apply the theory of rational generating functions to find a closed formula for a_n . First we need the roots of the denominator, which are 1 and 2, with multiplicities 2 and 1, respectively. Then the a_n are of the form

$$P_1(n)1^n + P_2(n)2^n,$$

where P_1 is a polynomial of degree 1 in n and P_2 is a constant. Hence, $a_n = (A+Bn)+C2^n$, for some constants A, B , and C . We find these constants by using the initial conditions.

$$\begin{aligned} A + C &= 2 \\ A + B + 2C &= 2 \\ A + 2B + 4C &= 3 \end{aligned}$$

This system gives $A = C = 1$ and $B = -1$. Hence, $a_n = 1 - n + 2^n$.

4.3 A non-linear recurrence: Catalan numbers

Consider the following path counting problem.

We have two types of steps: $U = (1, 1)$ and $D = (1, -1)$. In how many ways can we go from $(0, 0)$ to $(2n, 0)$ using these steps and without crossing the horizontal axis?

These paths are usually called *Dyck paths*. See Figure 2.

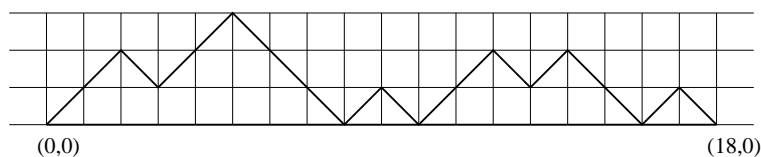


Figure 2: A Dyck path.

Let us denote by C_n the number of such paths. The first values of C_n can be computed by hand (Figure 3). Notice that $C_0 = 1$ since there is one way of going from $(0, 0)$ to $(0, 0)$.

We now look for a way of decomposing the paths so that we can obtain a recurrence (see Figure 4). Consider the first point where the path returns to the horizontal axis; this



Figure 3: Dyck paths of length at most 6.

point is of the form $(2i, 0)$ for some i with $1 \leq i \leq n$. Now our path is split into two smaller paths, one of length $2i$ and one of length $2(n-i)$. Observe that the first path, before the first return, can be decomposed as UPD , where P is a path that does not go below height 1. Hence the number of paths of length $2n$ whose first return is at $(2i, 0)$ is $C_{i-1}C_{n-i}$. Since the first return can be in any point of the form $(2i, 0)$ for i between 1 and n , we have that

$$C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-1}C_0 = \sum_{i=0}^{n-1} C_iC_{n-i-1},$$

which is valid for $n \geq 1$.

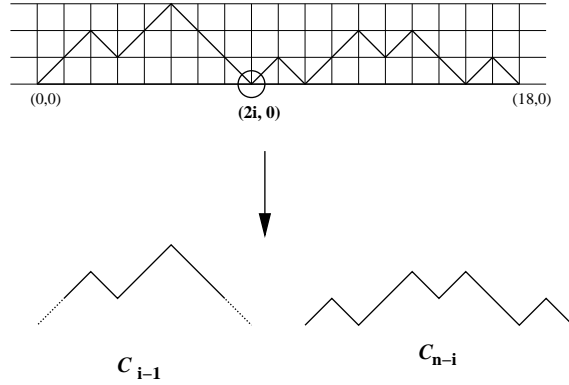


Figure 4: Decomposition of a Dyck path.

We change indices so that the recurrence is valid for $n \geq 0$:

$$C_{n+1} = \sum_{i=0}^n C_iC_{n-i},$$

and now we take generating functions:

$$\frac{C(z) - 1}{z} = C(z)^2.$$

Solving this quadratic equation on $C(z)$ we get

$$\frac{1 \pm \sqrt{1-4z}}{2z}.$$

Which of the two solutions are we interested in? Observe that the expansion of the term $\sqrt{1-4z}$ is $\sum_{n \geq 0} \binom{1/2}{n} (-4)^n z^n = 1 + \dots$. Therefore, if we take the $+$ sign above, the first term of $C(z)$ would be $1/z$, and this is not a power series. Hence we have to take the $-$ sign. So,

$$C(z) = \frac{1 - \sqrt{1-4z}}{2z}.$$

Now we want to extract the coefficient of z^n above to have a closed formula for C_n .

$$[z^n]C(z) = \frac{-1}{2}[z^{n+1}]\sqrt{1-4z} = \frac{-1}{2}(-4)^{n+1} \binom{1/2}{n+1}$$

Now,

$$\binom{1/2}{n+1} = \frac{\frac{1}{2} \cdot \frac{-1}{2} \cdots \frac{-2n+1}{2}}{(n+1)!} = \frac{(-1)^n}{4^n} \frac{(2n-1)!}{(n+1)!(n-1)!},$$

and finally

$$C_n = [z^n]C(z) = \frac{-1}{2}(-4)^{n+1} \frac{(-1)^n}{4^n} \frac{(2n-1)!}{(n+1)!(n-1)!} = \dots = \frac{1}{n+1} \binom{2n}{n}.$$

The numbers C_n are called *Catalan* numbers (although they first appeared in Euler's work). The first Catalan numbers are

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, \dots$$

We will see that Catalan numbers are one of the most ubiquitous in combinatorics since they count a very large variety of objects. The interested reader will find a challenge in exercise 6.19 of Stanley's *Enumerative Combinatorics, Volume 2*, where 66 different objects enumerated by Catalan numbers are given.

Observe finally that the generating function for Catalan numbers is not rational. Generating functions that satisfy a polynomial equation are called *algebraic*.

4.4 The generating function for integer partitions

Among all quantities we have studied, the number of partitions $p(n)$ seems to be one of the most out of reach. But its generating function will prove to us more tractable. Our goal is to find $\sum_{n \geq 0} p(n)z^n$. Let us start by a simple case. Let $p^{\leq k}(n)$ be the number of partitions of n all whose parts are k or less. We study first the GF for $p^{\leq 1}(n)$. Well, there is just one partition of n all whose parts are 1, hence

$$\sum_{n \geq 0} p^{\leq 1}(n)z^n = \frac{1}{1-z}.$$

For $k = 2$, we claim that

$$\sum_{n \geq 0} p^{\leq 2}(n) z^n = \frac{1}{1-z} \frac{1}{1-z^2}.$$

We first rewrite the RHS as

$$(1 + z + z^2 + z^3 + \cdots)(1 + z^2 + z^4 + z^6 + \cdots).$$

If we expand this product, we get terms of the form $z^i(z^2)^j$ for $0 \leq i, j$. This term is encoding a partition of $i + 2j$ all whose parts are at most 2; namely, the partition containing j 2's and i 1's. And all partitions arise in this way. Hence the claim is proved.

In the same way, one can prove that

$$\sum_{n \geq 0} p^{\leq 3}(n) z^n = \frac{1}{1-z} \frac{1}{1-z^2} \frac{1}{1-z^3}.$$

The powers of z count the parts that are 1, the powers of z^2 count parts that are 2, and the powers of z^3 count the parts that are 3.

How can we generalize this is we want to find the generating function for all partitions, without any restriction on the size of the parts? The obvious candidate now is

$$\sum_{n \geq 0} p(n) z^n = \frac{1}{1-z} \frac{1}{1-z^2} \frac{1}{1-z^3} \frac{1}{1-z^4} \cdots = \prod_{i \geq 1} \frac{1}{1-z^i}$$

But does this infinite product make sense in terms of formal power series? It does, as far as we understand that we pick only a *finite* number of terms that are different from 1.

Once we have understood how the generating function for partitions works, we can start “playing” with it. Let us prove a result we mentioned before.

Theorem 4.10. *The number of partitions of n into odd parts is the same as the number of partitions of n into different parts.*

Proof. We prove the equality by showing that the respective generating functions are equal. The generating function for partitions into odd parts is

$$o(z) = \frac{1}{1-z} \frac{1}{1-z^3} \frac{1}{1-z^5} \cdots = \prod_{i \geq 1} \frac{1}{1-z^{2i-1}}.$$

On the other hand, the generating function for partitions with different parts is

$$d(z) = (1+z)(1+z^2)(1+z^3) \cdots = \prod_{i \geq 1} (1+z^i),$$

since from each of the terms $1 + z^i + (z^i)^2 + (z^i)^3 + \cdots$ we can only pick either a 1 or a z^i .

Observe that $(1+z^i)(1-z^i) = (1-z^{2i})$. Hence,

$$d(z) = \prod_{i \geq 1} \frac{1-z^{2i}}{1-z^i} = \frac{1-z^2}{1-z} \frac{1-z^4}{1-z^2} \frac{1-z^6}{1-z^3} \frac{1-z^8}{1-z^4} \cdots = \prod_{i \geq 1} \frac{1}{1-z^{2i-1}} = o(z),$$

as required. □

5 The symbolic method for unlabelled structures

Now we have the tools to approach generating functions in a more systematic way. Our next goal is to provide a framework that allows us to find easily the generating functions for the combinatorial objects we are interested in, avoiding as much as possible setting up recurrences. Our approach mimics that of Flajolet and Sedgewick¹⁴, but due to time restrictions we will only scratch the surface of their powerful method. As it has been the case during all the course, we will develop most ideas by example. We need first to define the objects we will deal with.

Definition 5.1. A combinatorial class \mathcal{A} is a finite or denumerable set endowed with a size function $||$ such that

- for all $\alpha \in \mathcal{A}$, $0 \leq |\alpha| < \infty$;
- the number of elements of a given size is finite.

For a combinatorial class \mathcal{A} , its elements are denoted α and their sizes $|\alpha|$. For each $n \geq 0$, we denote by \mathcal{A}_n the set of elements of size n , and a_n is $|\mathcal{A}_n|$, that is, the number of elements of size n . We say that $\{a_n\}_{n \geq 0}$ is the *counting sequence* of the combinatorial class \mathcal{A} , and $a(z) = \sum_{n \geq 0} a_n z^n$ is the OGF of the class \mathcal{A} . Note the alternative definition of $a(z)$ as $a(z) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|}$. Let us get familiar with this concepts by examining some examples.

Example. Let $\mathcal{W}_{0,1}$ be the set of binary words, ie, words over the alphabet $\{0, 1\}$. So

$$\mathcal{W}_{0,1} = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots\},$$

where ϵ denotes the empty word (the word with no letter). Here the size of a word is the number of letters, hence w_n is the number of binary words with n letters. It is straightforward then that $w_n = 2^n$ and the corresponding generating function is $w(z) = \sum_{n \geq 0} 2^n z^n = \frac{1}{1-2z}$.

Example. Let \mathcal{P} be the set of all permutations of the set $[n]$. Hence,

$$\mathcal{P} = \{\epsilon, 1, 12, 21, 123, 132, 231, 213, 312, 321, \dots\}.$$

We know well that $p_n = |\mathcal{P}_n| = n!$, hence $p(z) = \sum_{n \geq 0} n! z^n$. Note here that $p(z)$, regarded as an analytic series, does not converge for any value of z except 0, but from our formal perspective this does not matter much.

Of course, our goal is to be able to find GF's for classes much more complicated than the ones described above, which we can already handle. Towards this aim, we need to introduce some operations on combinatorial classes that translate into operations on generating functions. In this way, from a very simple set of tools we will be able to study quite involved objects.

We first need to introduce two trivial combinatorial classes. One is the *neutral class*, that consists of a unique element ϵ that has size zero. We have also the *atomic class*, that contains a unique element ζ of size one. Their respective generating functions are, trivially, 1 and z .

¹⁴ *Analytic Combinatorics. Symbolic Combinatorics*, preliminary version available on-line, see footnote 11.

5.1 Constructions

Product. Let \mathcal{A} and \mathcal{B} be two combinatorial classes. Their *product* is defined as

$$\mathcal{C} = \mathcal{A} \times \mathcal{B} = \{\alpha\beta : \alpha \in \mathcal{A}, \beta \in \mathcal{B}\},$$

having as size function $|\alpha\beta| = |\alpha| + |\beta|$. (For notational economy, we write $\alpha\beta$ instead of (α, β) .)

Example. Consider the classes $\mathcal{W}_{0,1}$ of binary words over $\{0, 1\}$ and $\mathcal{W}_{a,b}$ of binary words over $\{a, b\}$, where in both the size of an object is the number of letters of the word. Their product has as elements

$$\mathcal{W}_{0,1} \times \mathcal{W}_{a,b} = \{\epsilon\epsilon, \epsilon a, \epsilon b, 0\epsilon, 1\epsilon, 0a, 0b, 1a, 1b \dots\};$$

we actually lighten notation by dropping the ϵ 's

$$\mathcal{W}_{0,1} \times \mathcal{W}_{a,b} = \{\epsilon, a, b, 0, 1, 0a, 0b, 1a, 1b \dots\}.$$

Suppose now that we are given the GF's $a(z)$ and $b(z)$ for \mathcal{A} and \mathcal{B} ; our aim is to give the GF for $\mathcal{A} \times \mathcal{B}$.

$$c(z) = \sum_{\gamma \in \mathcal{C}} z^{|\gamma|} = \sum_{\alpha\beta \in \mathcal{A} \times \mathcal{B}} z^{|\alpha\beta|} = \sum_{\alpha\beta \in \mathcal{A} \times \mathcal{B}} z^{|\alpha|+|\beta|} = \left(\sum_{\alpha \in \mathcal{A}} z^{|\alpha|} \right) \left(\sum_{\beta \in \mathcal{B}} z^{|\beta|} \right) = a(z)b(z)$$

Hence we have proved the following.

Proposition 5.2. *The generating function for the product of two classes is the product of their generating functions.*

Example. Let us continue with the example of $\mathcal{W}_{0,1}$ and $\mathcal{W}_{a,b}$. Their respective generating functions are

$$w_{0,1}(z) = w_{a,b}(z) = \frac{1}{1-2z};$$

therefore, the generating function for the product $W = \mathcal{W}_{0,1} \times \mathcal{W}_{a,b}$ is

$$\left(\frac{1}{1-2z} \right)^2 = \sum_{n \geq 0} \binom{-2}{n} (-2)^n z^n.$$

By expanding the binomial coefficient,

$$\binom{-2}{n} = \frac{(-2)(-3)(-4) \cdots (-2-n+1)}{n!} = (-1)^n \frac{(n+1)!}{n!} = n+1.$$

Hence,

$$w(z) = \sum_{n \geq 0} (n+1) 2^n z^n.$$

You may argue that we took a long route to get to something not that difficult to prove. Indeed, there are $(n + 1)2^n$ words of length n that start with 0 and 1 and then continue with a and b : pick any of the 2^n words over $\{0, 1\}$ and decide from which of the $n + 1$ positions we switch 0's to a 's and 1's to b 's. Hopefully, our next examples will show the real power of the symbolic method.

Sum. Suppose again that \mathcal{A} and \mathcal{B} are two combinatorial classes; furthermore, assume they are disjoint (if they are not, work with $\mathcal{A} \times \epsilon_1$ and $\mathcal{B} \times \epsilon_2$). Their sum is defined as

$$\mathcal{C} = \mathcal{A} + \mathcal{B} = \{\gamma : \gamma \in \mathcal{A} \cup \mathcal{B}\}.$$

The size of an element γ is the size it had originally. The generating function for the sum is, not surprisingly, the sum of the generating functions.

$$c(z) = \sum_{\gamma \in \mathcal{A} + \mathcal{B}} z^{|\gamma|} = \sum_{\gamma \in \mathcal{A}} z^{|\gamma|} + \sum_{\gamma \in \mathcal{B}} z^{|\gamma|} = a(z) + b(z).$$

Proposition 5.3. *The generating function of the sum of two classes is the sum of the respective generating functions.*

Now that we have sums and products, we can study more involved objects.

Example. (Triangulations of a polygon.) Given a regular n -gon, we are interested in counting the number of triangulations it has. Let us denote by \mathcal{T} the combinatorial class of triangulations of polygons, where the size of a triangulation is the number of triangles it has. Then $t_0 = 1$, $t_1 = 1$, $t_2 = 2$ and $t_3 = 5$ (see Figure 5). (Do these numbers sound familiar?)

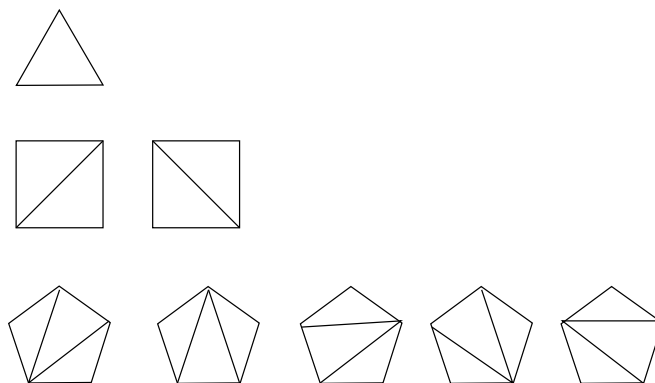


Figure 5: Polygon triangulations.

Consider that the vertices of an n -gon are labelled 1 to n counterclockwise. We can decompose a triangulation as follows. Consider the triangle that contains the side 12; this we call the *root* triangle. To the left and right of the root triangle, the polygon is split into two smaller polygons (which may consist of just one side). Each of these two smaller polygons is triangulated in turn (see Figure 6).

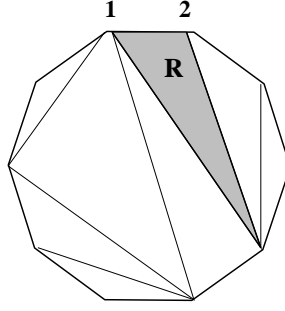


Figure 6: Decomposition of a polygon triangulation.

Hence, a triangulation of a polygon is either empty (if the polygon is just an edge), or can be decomposed as a triangulation, followed by a root triangle, followed by another triangulation. Therefore,

$$\mathcal{T} = \epsilon + \mathcal{T}\zeta\mathcal{T},$$

where ζ denotes the root triangle. Now we can translate this combinatorial specification into generating functions:

$$t(z) = 1 + t(z)zt(z).$$

Hence, $t(z)$ satisfies the equation $t(z) = 1 + zt(z)^2$, which we solve and get $t(z) = \frac{1 - \sqrt{1 - 4z}}{2z}$. Hence Catalan numbers again! (Actually, this derivation was first made by the Swiss Leonard Euler, but the numbers bear the name of the Belgian Eugène Catalan). This is an example of a *recursive* specification of a combinatorial class, since we expressed the class \mathcal{T} in terms of itself.

Sequence. Let \mathcal{A} be a combinatorial class. The *sequence* of \mathcal{A} is the class defined by

$$\mathcal{S}(\mathcal{A}) = \epsilon + \mathcal{A} + \mathcal{A} \times \mathcal{A} + \mathcal{A} \times \mathcal{A} \times \mathcal{A} + \dots$$

Is it indeed a combinatorial class? How many objects there are of size n ? To count objects of size n in $\mathcal{S}(\mathcal{A})$, we need to know how many objects of size n there are in $\mathcal{A}^i = \mathcal{A} \times \dots \times \mathcal{A}$. The size of an object in \mathcal{A}^i is the sum of the sizes of its i components. If all objects in \mathcal{A} have size at least one, then the objects in \mathcal{A}^i have size at least i , and hence the terms of the form \mathcal{A}^j for $j > n$ never give rise to objects of size n . Thus, there is only a finite number of objects of size n . But note that if there are objects in \mathcal{A} of size 0, then we may have objects of size n in all of \mathcal{A}^i , so in total an infinite number of them, contradicting the definition of combinatorial class. Therefore, we only consider the sequence construction of classes that do not have elements of size zero.

Now for the generating function; by applying the rules for sums and products we obtain

$$s(z) = 1 + a(z) + a(z)^2 + a(z)^3 + \dots = \frac{1}{1 - a(z)}.$$

Proposition 5.4. *The generating function for the sequence of a class whose generating function is $a(z)$ is $\frac{1}{1 - a(z)}$.*

Example. Let us examine again the simple example of binary words over $\{0, 1\}$. Such a word is nothing but a sequence of 0's and 1's. Hence,

$$\mathcal{W}_{0,1} = \mathcal{S}(\{0, 1\}) \Rightarrow w(z) = \frac{1}{1 - 2z},$$

since the GF for the class $\{0, 1\}$ is $2z$.

Example. Consider the class \mathcal{U} of words over $\{0, 1\}$ that do not have k consecutive zeros. Let us start by the case $k = 2$. A word in \mathcal{U} can end in 1 or 0, but if it ends in 0 the previous letter must be 1 (unless the word is the word 0), so we can say that words in \mathcal{U} end in either 1 or 10. Hence the following equation holds

$$\mathcal{U} = \epsilon + \{0\} + \mathcal{U} \times \{1\} + \mathcal{U} \times \{10\}.$$

Translating this into GF's,

$$u(z) = 1 + z + zu(z) + z^2u(z) \Rightarrow u(z) = \frac{1 + z}{1 - z - z^2},$$

which is almost like the GF for Fibonacci numbers, except that the denominator has an extra power of z . If now we want to consider the case of not having k consecutive zeros, the possible endings of a word are 1, 10, 100, ..., $10 \cdots 0$, where this last word has $k - 1$ zeros at the end; in addition we have to consider the cases of words of length less than k consisting only of 0's. Hence,

$$\mathcal{U} = \epsilon + \{0\} + \{00\} + \cdots + \{0 \cdots 0\} + \mathcal{U} \times \{1\} + \mathcal{U} \times \{10\} + \mathcal{U} \times \{100\} + \cdots + \mathcal{U} \times \{10 \cdots 0\}.$$

And for the generating function,

$$u(z) = 1 + z + z^2 + \cdots + z^{k-1} + (z + z^2 + z^3 + \cdots + z^k)u(z);$$

hence,

$$u(z) = \frac{1 + z + \cdots + z^{k-1}}{1 - z - z^2 - \cdots - z^k}.$$

The coefficients of these generating function can be seen as a generalization of Fibonacci numbers.

Let us examine another way of treating the class \mathcal{U} . We can think of a word with no k consecutive 0's as a sequence of 1's, each followed by at most $k - 1$ 0's. This gives

$$\mathcal{U} = \{\epsilon + 0 + 00 + \cdots + 0 \overset{(k-1)}{\cdots} 0\} \mathcal{S}(1 \times \{\epsilon + 0 + 00 + \cdots + 0 \overset{(k-1)}{\cdots} 0\}).$$

Translating into GF's,

$$u(z) = (1 + z + \cdots + z^{k-1}) \frac{1}{1 - z(1 + z + \cdots + z^{k-1})},$$

which leads again to the same generating function, of course.

There are other constructions for combinatorial classes, but for our purposes sums, products, and sequences suffice.

5.2 Compositions revisited

Let \mathcal{C} be the class of integer compositions, where a composition of n has weight n . Recall that we can represent a composition as a dots and bars diagram; for instance, the composition $2 + 1 + 3 + 1$ of 7 will look like

$$\bullet\bullet \mid \bullet \mid \bullet\bullet\bullet \mid \bullet.$$

From this representation we see that a composition is a sequence of strictly positive integers. So, $\mathcal{C} = \mathcal{S}(\mathcal{I})$, where \mathcal{I} is the class of strictly positive integers. To derive the GF for compositions, we need first the GF for \mathcal{I} . One of the many ways of doing this is thinking that an integer is a sequence of dots, each with weight 1; since we only want positive integers, we have $\mathcal{I} = \mathcal{S}(\bullet) - \epsilon$. Hence,

$$i(z) = \frac{1}{1-z} - 1 = \frac{z}{1-z}.$$

Now for the compositions, $\mathcal{C} = \mathcal{S}(\mathcal{I})$ implies

$$c(z) = \frac{1}{1 - \frac{z}{1-z}} = \frac{1-z}{1-2z}.$$

From this is easy to recover the result that $c(n) = 2^{n-1}$. Indeed,

$$\frac{1-z}{1-2z} = \frac{1}{1-2z} - \frac{z}{1-2z} = \sum_{n \geq 0} 2^n z^n - z \sum_{n \geq 0} 2^n z^n = 1 + \sum_{n \geq 1} 2^{n-1} z^n.$$

So far not very surprising...

Imagine now that instead of counting general compositions, we want to restrict to those whose parts are only 1 and 2; let us call this class $\mathcal{C}_{1,2}$. It should be clear that $\mathcal{C}_{1,2} = \mathcal{S}(\bullet, \bullet\bullet)$. The GF for the class $\{\bullet, \bullet\bullet\}$ is $z + 2z^2$, and hence the GF for compositions with parts 1 or 2 is

$$c_{1,2}(z) = \frac{1}{1 - z - z^2}.$$

Recall that this is the GF for Fibonacci numbers (as an exercise, show that compositions whose parts are 1 and 2 satisfy the recurrence for Fibonacci numbers). In general, if we want compositions whose parts are $\{p_1, p_2, \dots, p_r\}$, the generating function will be

$$\frac{1}{1 - z^{p_1} - z^{p_2} - \dots - z^{p_r}}.$$

Let us study in some detail the case of parts $\{1, 2, 3\}$. The generating function is

$$\frac{1}{1 - z - z^2 - z^3}.$$

Imagine that we do not need the exact form of the coefficients, but rather want to have an idea about their order of magnitude. Since the generating function is rational, we can apply Theorem 4.9. First we compute the roots of the denominator; in this case, $r_1 \sim 0.5437$,

$r_2 \sim -.7718 + i1.1151$, and $r_3 \sim -.7718 - i1.1151$. Since each root has multiplicity one, we know that

$$\frac{1}{1 - z - z^2 - z^3} = A \sum_{n \geq 0} \left(\frac{1}{r_1}\right)^n z^n + B \sum_{n \geq 0} \left(\frac{1}{r_2}\right)^n z^n + C \sum_{n \geq 0} \left(\frac{1}{r_3}\right)^n z^n$$

for some constants A, B, C . Since $|1/r_1| \sim 1.8393$ and $|1/r_2| = |1/r_3| \sim 0.7374$, for large n the term $(1/r_1)^n$ will “win” over the others. Hence, we can say that the number of compositions of n with parts 1, 2, 3 behaves asymptotically as $A1.8393^n$, for some constant A . The exact value of the constant could be found without much difficulty if we are interested.

From this example we can extract the following principle. If $a(z)$ is a rational generating function and γ is the root of the denominator that has smallest absolute value, and γ is a simple root, then for large n

$$[z^n]a(z) \sim c \left(\frac{1}{\gamma}\right)^n$$

for some constant c .

5.3 Rooted plane trees

A *tree* is a connected acyclic graph; if a tree has n vertices, it is well-known that it has $n - 1$ edges. A *rooted tree* is a tree that has a distinguished vertex, the *root*. A rooted tree is *plane* if we consider it embedded in the plane, that is, the relative order of the subtrees that hang from each vertex is relevant. The following figure shows all rooted plane trees up to 4 vertices (contrary to real trees, the root is the topmost vertex).

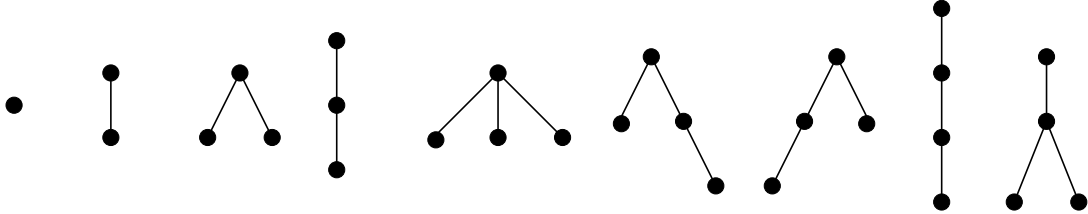


Figure 7: Rooted plane trees.

Our first goal will be to count rooted plane trees according to their number of vertices. Observe that we can define them recursively as follows: a plane rooted tree consists of a vertex from which hangs a (possibly empty) ordered set of plane rooted trees. In the language of combinatorial classes,

$$\mathcal{T} = \zeta \times \mathcal{S}(\mathcal{T}).$$

Hence,

$$t(z) = z \frac{1}{1 - t(z)} \Rightarrow t(z)^2 - t(z) + z = 0.$$

Solving this equation we get the somewhat familiar generating function

$$t(z) = \frac{1 - \sqrt{1 - 4z}}{2}.$$

Indeed, this is the GF for Catalan numbers multiplied by z . Hence, t_n , the number of rooted plane trees with n vertices, is the $(n - 1)$ -rst Catalan number, $C_{n-1} = \frac{1}{n} \binom{2n-2}{n-1}$.

Let us consider now *binary* rooted plane trees. That is, rooted plane trees where from each vertex hang either two or zero subtrees. The vertices that have two subtrees are called *internal* vertices, and the terminal vertices are called *leaves*. It is not difficult to show that the number of leaves is the number of internal vertices plus one. One usually counts binary rooted plane trees according to the number of internal vertices. So let \mathcal{U} be the class of binary rooted plane trees with the size function being the number of internal vertices. A member of \mathcal{U} is then either just a root (size zero) or a root from which hangs a pair of trees from \mathcal{U} . Hence,

$$\mathcal{U} = \epsilon + \zeta \times \mathcal{U} \times \mathcal{U}.$$

Taking generating functions,

$$u(z) = 1 + zu(z)^2,$$

which, again!, is the GF for Catalan numbers. So the number of binary trees with n internal vertices is C_n . Find a bijection between binary rooted plane trees with n internal vertices and rooted plane trees with $n + 1$ vertices.

In general, we can consider rooted plane trees where the outdegree of each vertex belongs to a set of integers $\Omega \subseteq \mathbb{N}$ (which has to include always 0). If we denote by \mathcal{U}_Ω the class of such trees, with the size of a tree being again the number of internal vertices, a moment's thought gives the following equation

$$\mathcal{U}_\Omega = \epsilon + \zeta \times \left(\sum_{w \in \Omega \setminus 0} \mathcal{U}_\Omega^w \right),$$

which translates to GF's as

$$u(z) = 1 + z \left(\sum_{w \in \Omega \setminus 0} u(z)^w \right).$$

If instead of counting according to the number of internal vertices we want to count trees with respect to the total number of vertices, and with the out-degrees still restricted to Ω , we have the following equation

$$\mathcal{T}_\Omega = \zeta \times \left(\epsilon + \sum_{w \in \Omega \setminus 0} \mathcal{T}_\Omega^w \right),$$

and this gives, in terms of generating functions,

$$t(z) = z \left(1 + \sum_{w \in \Omega \setminus 0} t(z)^w \right).$$

6 The symbolic method for labelled structures

The combinatorial classes we have dealt with so far were “unlabelled”, in the sense that the pieces or atoms that make up an object were undistinguishable among them and bear no particular label or tag. At this point we are interested in enumerating labelled objects, such as:

- Set partitions, where each atom is an integer from 1 to n .
- Labelled graphs, where each vertex has a label, usually an integer. Hence, we regard the two graphs in Figure 8 as different.

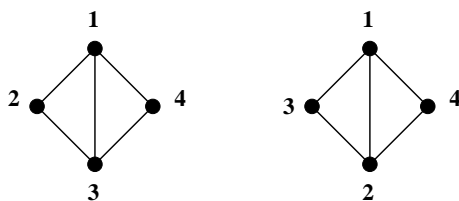


Figure 8: Two different labelled graphs.

Definition 6.1. A combinatorial class is labelled if it is a class and each object is labelled in the following sense: if an object has size n , then it bears n different labels belonging to the set $[n]$.

So, in a labelled class, the size of an object and the number of labels are always equal. Let us look at some examples.

Example. Graphs are a very natural labelled class. In a graph with n vertices, we label them with the integers from 1 to n . Observe that not all graphs with n vertices can be labelled in the same number of ways. For instance, a complete graph can only be labelled in one way, whereas a graph with n vertices and only one edge can be labelled in $\binom{n}{2}$ ways.

Example. Set partitions of $[n]$ are a labelled class.

Example. Permutations of $[n]$ are also a labelled class. Its objects can be described as sequences of labeled atoms.

As with unlabelled classes, we have an empty class $\{\epsilon\}$ whose only element has size 0 and hence bears no label. We also have the atomic class ζ that has a unique element of size 1 and bearing the label 1.

To enumerate labelled classes we have to introduce a new kind of generating function, the exponential generating function (EGF). As before, let a_n denote the number of objects of size n in the labelled class \mathcal{A} . The *exponential generating function* for \mathcal{A} is

$$a(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!} = \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!}.$$

The name “exponential” comes of course from the fact that $\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}$.

Example. Let \mathcal{P} be the class of permutations. Its EGF is

$$p(z) = \sum_{n \geq 0} n! \frac{z^n}{n!} = \sum_{n \geq 0} z^n = \frac{1}{1-z}.$$

6.1 Constructions

As we did with unlabelled classes, we define constructions on classes that translate to operations in the corresponding exponential generating functions.

Sum. It works exactly the same as with unlabelled classes. Given two disjoint labelled combinatorial classes \mathcal{A} and \mathcal{B} , their sum is the class $\mathcal{C} = \mathcal{A} + \mathcal{B} = \{\gamma : \gamma \in \mathcal{A} \cup \mathcal{B}\}$, where the size and the labels of an object are inherited from either \mathcal{A} or \mathcal{B} . The corresponding EGF is again the sum of the EGF’s of the summands.

Product. The product of two labelled classes has to be defined precisely, since we have to take care of the labels. Let \mathcal{A} and \mathcal{B} be two labelled classes and let $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$. The element (α, β) in the cartesian product $\mathcal{A} \times \mathcal{B}$ should have size $|\alpha| + |\beta|$, as before, and hence should be labelled with the integers from 1 to $|\alpha| + |\beta|$. If we do not modify the labels, this is not achieved, since they will be repeated labels and they will run only to $\max\{|\alpha|, |\beta|\}$. Here is how we surpass this difficulty.

Given a labelled object γ , say that γ' is a *relabelling* of γ if γ and γ' agree as unlabelled structures and the labels of γ' have the same relative order as the ones of γ (but do not necessarily consist of the integers from 1 to $|\gamma|$). Here’s an example. Consider graph G in Figure 9. The graph G' is a relabelling of G because the smallest label, 3, replaces 1 in G , the second smallest, 12, replaces 2, and so on. But H is not a relabelling of G since the two largest labels are not linked by an edge. We write $\rho(\gamma') = \gamma$ to denote the fact that γ' is a relabelling of γ (one also says that γ' *reduces* to γ).

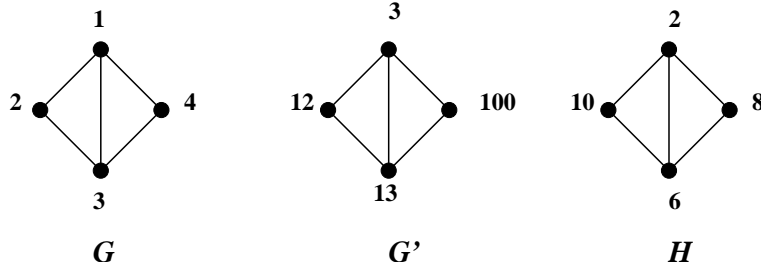


Figure 9: G' is a relabelling of G , whereas H is not

With the notion of relabelling we can now define the labelled product of two objects:

$$\alpha \star \beta = \{(\alpha', \beta') : (\alpha', \beta') \text{ is well labelled and } \rho(\alpha') = \alpha, \rho(\beta') = \beta\}$$

So, the labelled product of two objects is not a single object, but a collection of labelled objects. Actually, it is easy to see that if $|\alpha| = i$ and $|\beta| = j$, then $\alpha \star \beta$ has $\binom{i+j}{i}$ elements. Let us see how the labelled product works with an example.

Example. Consider the two labelled rooted plane trees in Figure 10; each is labelled with the integers $\{1, 2\}$. Their product is the set of six pairs of trees labelled with the integers $\{1, 2, 3, 4\}$.

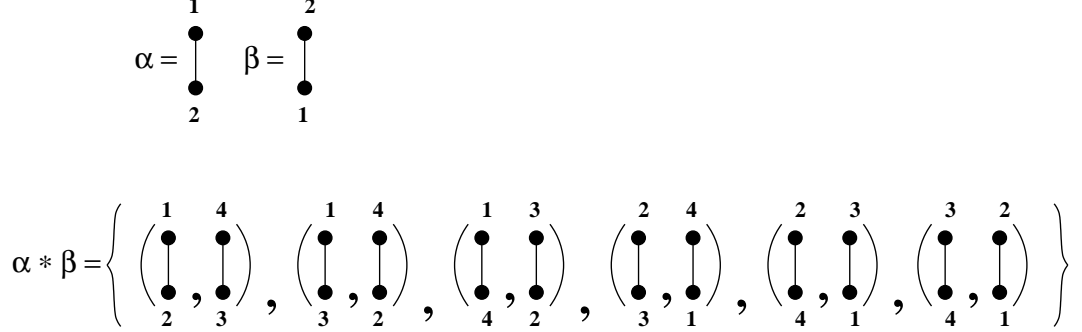


Figure 10: The labelled product of two rooted trees

Now that we have defined the labelled product of two elements, we can define the labelled product of two labelled classes:

$$\mathcal{A} \star \mathcal{B} = \bigcup_{\alpha \in \mathcal{A}, \beta \in \mathcal{B}} \alpha \star \beta.$$

The next goal is to find the EGF for the labelled product. Let c_n denote the number of elements of size n in $\mathcal{A} \star \mathcal{B}$. Each element counted in c_n is a pair consisting of an element from \mathcal{A} of size i and an element of \mathcal{B} of size $n - i$, and this pair relabelled in any consistent way. But, as observed above, such a pair can be relabelled in $\binom{n}{i}$ ways. Hence,

$$c_n = \sum_{i=0}^n a_i b_{n-i} \binom{n}{i}.$$

Therefore,

$$\begin{aligned} c(z) &= \sum_{n \geq 0} c_n \frac{z^n}{n!} = \sum_{n \geq 0} \left(\sum_{i=0}^n a_i b_{n-i} \binom{n}{i} \right) \frac{z^n}{n!} = \sum_{n \geq 0} \left(\sum_{i=0}^n \frac{a_i}{i!} \frac{b_{n-i}}{(n-i)!} \right) z^n \\ &= \left(\sum_{n \geq 0} a_n \frac{z^n}{n!} \right) \left(\sum_{n \geq 0} b_n \frac{z^n}{n!} \right) = a(z)b(z). \end{aligned}$$

Thus, the exponential generating function of the product of two labelled classes is the product of the corresponding exponential generating functions.

Once we have the product, the sequence construction works the same as in the unlabelled case.

$$\mathcal{S}(\mathcal{A}) = \epsilon + \mathcal{A} + \mathcal{A} \star \mathcal{A} + \mathcal{A} \star \mathcal{A} \star \mathcal{A} + \dots$$

Where, as in the unlabelled case, we only consider this constructions for classes that do not have elements of size 0. Taking EGF's, we get that the EGF for the sequence construction is

$$s(z) = 1 + a(z) + a(z)^2 + a(z)^3 + \cdots = \frac{1}{1 - a(z)}.$$

Example. Consider again the class \mathcal{T} of labelled rooted plane trees, where the size of a tree is the number of vertices. As before, a tree consists of a root, of size 1, together with a sequence of labelled rooted plane trees. Hence,

$$\mathcal{T} = \zeta \star \mathcal{S}(\mathcal{T}) \Rightarrow t(z) = z \frac{1}{1 - t(z)}.$$

Therefore the EGF for labelled rooted plane trees is the same as the OGF of rooted plane trees; but this does not mean that there are as many labelled trees as unlabelled ones. The number of labelled rooted plane trees is

$$n![z^n]t(z) = n! \frac{1}{n} \binom{2n-2}{n-1} = \frac{(2n-2)!}{(n-1)!}.$$

Suppose now that we want to count labelled rooted trees, without the planarity requirement. Hence, the order of the subtrees that hang from each vertex does not matter. We can no longer say that such a tree is a root together with a sequence of trees; rather, we would like to say that we have a root together with a “set” of trees. Let us formalize the concept of a set of a labelled class.

Let $\mathcal{P}^k(\mathcal{A})$ denote the class obtained by taking sets of k elements of \mathcal{A} . By this we mean that we take the product of k copies of \mathcal{A} and we regard two elements $(\alpha_1, \dots, \alpha_k)$ and $(\alpha'_1, \dots, \alpha'_k)$ as the same if for some permutation π of $[k]$, we have that $(\alpha_{\pi(1)}, \dots, \alpha_{\pi(k)}) = (\alpha'_1, \dots, \alpha'_k)$. That is, we consider the product of k copies of \mathcal{A} regardless of the order of the components. Since each element in \mathcal{A}^k can be ordered in $k!$ ways, we have that the EGF for $\mathcal{P}^k(\mathcal{A})$ is

$$p^k(z) = \frac{a(z)^k}{k!}.$$

Now let $\mathcal{P}(\mathcal{A})$ denote the class of all subsets of \mathcal{A} , including the empty set. Hence,

$$\mathcal{P}(\mathcal{A}) = \epsilon + \mathcal{A} + \mathcal{P}^2(\mathcal{A}) + \mathcal{P}^3(\mathcal{A}) + \cdots$$

And for the EGF,

$$p(z) = 1 + a(z) + \frac{a(z)^2}{2!} + \frac{a(z)^3}{3!} + \cdots = \exp(a(z)).$$

So, the set construction translates to taking the exponential of the EGF.

6.2 Labelled graphs

Now we can easily solve the problem of labelled rooted trees (non-plane). A labelled rooted tree consists of a root ζ from which hangs a set of rooted trees. Hence,

$$\mathcal{T} = \zeta \star \mathcal{P}(\mathcal{T})$$

and taking EGF's

$$t(z) = z \exp(t(z)).$$

The problem that arises now is to solve this equation. It is not the first implicit equation that we encounter in this course, but the previous ones, like for Catalan numbers, were easy enough to solve by hand. An extremely useful tool in this sort of situations is Lagrange's inversion formula.

Theorem 6.2. *Let $Y = z\Phi(Y)$ be an implicit equation for the formal power series Y , in the variable z . Assume that Φ is also a formal power series and that $\Phi(0) = 1$. Then*

$$[z^n]Y(z) = \frac{1}{n}[u^{n-1}]\Phi(u)^n.$$

Proof. One proof follows from the analogous result in analysis. There are proofs purely in terms of formal power series; they use a bit of the spirit of complex analysis. See for instance the appendix in Van Lint and Wilson¹⁵. \square

Let us see how Lagrange's inversion formula works for our equation $t(z) = z \exp(t(z))$. In this case, Φ is \exp . Hence,

$$[z^n]t(z) = \frac{1}{n}[u^{n-1}](\exp(u))^n = \frac{1}{n}[u^{n-1}](\exp(nu)),$$

by the properties of the exponential. But the coefficient of u^{n-1} in $\exp(nu)$ is $\frac{n^{n-1}}{(n-1)!}$. Hence, $[z^n]t(z) = \frac{n^{n-1}}{n!}$. Recall that $t(z)$ is an exponential generating function, hence the number of rooted trees is not the coefficient of z^n , but $n!$ times this coefficient. Hence the total number of labelled rooted trees is n^{n-1} .

Imagine now that we just want labelled trees, regardless of the root. For each labelled unrooted tree with n vertices, we have n choices for the root. Hence, the number of labelled trees is $n^{n-1}/n = n^{n-2}$. This is in fact a famous theorem of Cayley, that perhaps you know from a graph theory course. This is not the most common proof of Cayley's theorem; there exist more combinatorial proofs, one of the most popular using Prüfer sequences¹⁶.

Now we can even move from trees to general labelled graphs. Let \mathcal{G} denote the class of labelled graphs, with the size being the number of vertices. If a graph has n labelled vertices, it can have as edges any subset of the $\binom{n}{2}$ possible edges. Hence, there are $2^{\binom{n}{2}}$

¹⁵ *A course in combinatorics*, Cambridge UP.

¹⁶ Most graph theory textbooks contain this proof. The book *Proofs from the book* by Aigner and Ziegler (Springer) contains half a dozen nice proofs of Cayley's theorem.

labelled graphs on n vertices. Since each unlabelled graph can be labelled in at most $n!$ ways, there are at most $\frac{1}{n!}2^{\binom{n}{2}}$ unlabelled graphs on n vertices¹⁷. The EGF for \mathcal{G} is

$$g(z) = \sum_{n \geq 0} \frac{2^{\binom{n}{2}}}{n!} z^n.$$

Suppose that now we want to restrict to *connected* graphs. Since a graph is a set of connected components, we have that

$$\mathcal{G} = \mathcal{P}(\mathcal{K}),$$

where \mathcal{K} is the class of connected labelled graphs. Hence, for the EGF's,

$$g(z) = \exp(k(z)) \Rightarrow k(z) = l(g(z) - 1),$$

where $l(z)$ is the series $\sum_{n \geq 1} (-1)^{n-1} z^n / n$, that is, $\log(1 - z)$.

6.3 Set partitions revisited

Recall that a partition of the set $[n]$ is a decomposition of $[n]$ as the union of non-empty disjoint sets, each of them called a block. Let $\mathcal{A}^{(r)}$ the class of set partitions into r blocks, with the size being the number of elements in the set; it is a labelled class. A set partition into r blocks consists of a set of r non-empty sets of atoms. So let us study first the class \mathcal{V} of non-empty sets. It should be clear that

$$\mathcal{V} = \mathcal{P}^1(\zeta) + \mathcal{P}^2(\zeta) + \mathcal{P}^3(\zeta) + \dots$$

Then,

$$\mathcal{A}^{(r)} = \mathcal{P}^r(\mathcal{V}).$$

Taking EGF's,

$$v(z) = \exp(z) - 1, \quad a^{(r)}(z) = \frac{v(z)^r}{r!} = \frac{(\exp(z) - 1)^r}{r!}.$$

So $a(z)^{(r)}$ is the exponential generating function for Stirling numbers of the second kind $\left\{ \begin{smallmatrix} n \\ r \end{smallmatrix} \right\}$, for fixed r . By extracting the coefficient of z^n above we recover the formula for Stirling numbers of the second kind.

Recall that Bell numbers count the total number of partitions of the set $[n]$. Let \mathcal{B} be the class of partitions of $[n]$, regardless of the number of blocks. Hence, a member of \mathcal{B} is a set of non-empty sets of atoms.

$$\mathcal{B} = \mathcal{P}(\mathcal{V}) \Rightarrow b(z) = \exp(\exp(z) - 1),$$

which is the EGF for Bell numbers. By extracting the coefficient of z^n we get a formula for B_n as an infinite sum.

$$B_n = n! [z^n] \exp(\exp(z) - 1) = \frac{n!}{e} [z^n] \exp(\exp(z)) = \frac{n!}{e} [z^n] \sum_{k \geq 0} \frac{\exp(kz)}{k!} = \frac{1}{e} \sum_{k \geq 0} \frac{k^n}{n!}.$$

¹⁷Actually, this is the right number asymptotically, this was first proved by Pólya. Roughly speaking, it means that almost all graphs on n vertices can be labelled in $n!$ ways.

Alternatively, recall that Bell numbers can be expressed as a double finite sum using the formula for Stirling numbers of the second kind.

Recall the expansions of the hyperbolic sine and cosine:

$$\begin{aligned}\sinh(z) &= \sum_{i \geq 0} \frac{z^{2i+1}}{(2i+1)!} \\ \cosh(z) &= \sum_{i \geq 0} \frac{z^{2i}}{(2i)!}\end{aligned}$$

Use these expansions and the symbolic method to prove the entries in the following table.

<i>Set partitions</i>	Any number of blocks	Odd number of blocks	Even number of blocks
Any block sizes	$\exp(\exp(z) - 1)$	$\sinh(\exp(z) - 1)$	$\cosh(\exp(z) - 1)$
Odd block sizes	$\exp(\sinh(z))$	$\sinh(\sinh(z))$	$\cosh(\sinh(z))$
Even block sizes	$\exp(\cosh(z) - 1)$	$\sinh(\cosh(z) - 1)$	$\cosh(\cosh(z) - 1)$

6.4 Permutation decompositions revisited

Let \mathcal{Q} denote the class of permutations. We know well that its EGF is given by $1/(1-z)$. If we wish, we can prove this in terms of the symbolic method by saying that a permutation is a sequence of labeled atoms, so $\mathcal{Q} = \mathcal{S}(\zeta)$, from which the EGF follows immediately. Another way of looking at permutations is using cycle decompositions. Now, a permutation is a set of cycles, where by a cycle we mean a cyclic permutation. Hence, $\mathcal{Q} = \mathcal{P}(\mathcal{Z})$, where \mathcal{Z} denotes the class of cycles. The EGF for cycles is quite easy, given that there are $(n-1)!$ cycles of length n . It is $\sum_{n \geq 1} z^n/n$, which we denote by $\log(1/(1-z))$. Hence,

$$q(z) = \exp\left(\log\left(\frac{1}{1-z}\right)\right) = \frac{1}{1-z},$$

which of course is no surprise. As with set partitions, we can first find the EGF for Stirling numbers of the first kind.

$$\mathcal{Q}^{(k)} = \mathcal{P}^k(\mathcal{Z}) \Rightarrow q^{(k)}(z) = \sum_{n \geq 0} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} = \frac{1}{k!} \left(\log\left(\frac{1}{1-z}\right)\right)^k$$

An *involution* is a permutation π such that π^2 is the identity. Clearly the only cycle lengths allowed in the disjoint cycle decomposition of π are 1 and 2. Hence, $\mathcal{I} = \mathcal{P}((1) + (12))$, which implies that the corresponding EGF is $\exp(z + z^2/2)$; a formula can be easily derived from this expression.

We can also use the symbolic specification to find a new proof of an old result. Let \mathcal{D} be the class of derangements, that is, the class of permutations with no fixed points. Clearly, π is a derangement if and only if it contains no cycles of length 1 in its disjoint cycle decomposition. Therefore, $\mathcal{D} = \mathcal{P}(\mathcal{Z} - \zeta)$; hence, the EGF for derangements is

$$d(z) = \exp\left(\log\left(\frac{1}{1-z}\right) - z\right) = \frac{\exp(-z)}{1-z}.$$

It is easy to deduce from here the formula for the number of derangements of n that we found in the second chapter.