# Introduction to Combinatorics

## Course Notes for MATH 239

U. Waterloo C&O Department

PUBLISHED BY PUBLISHER

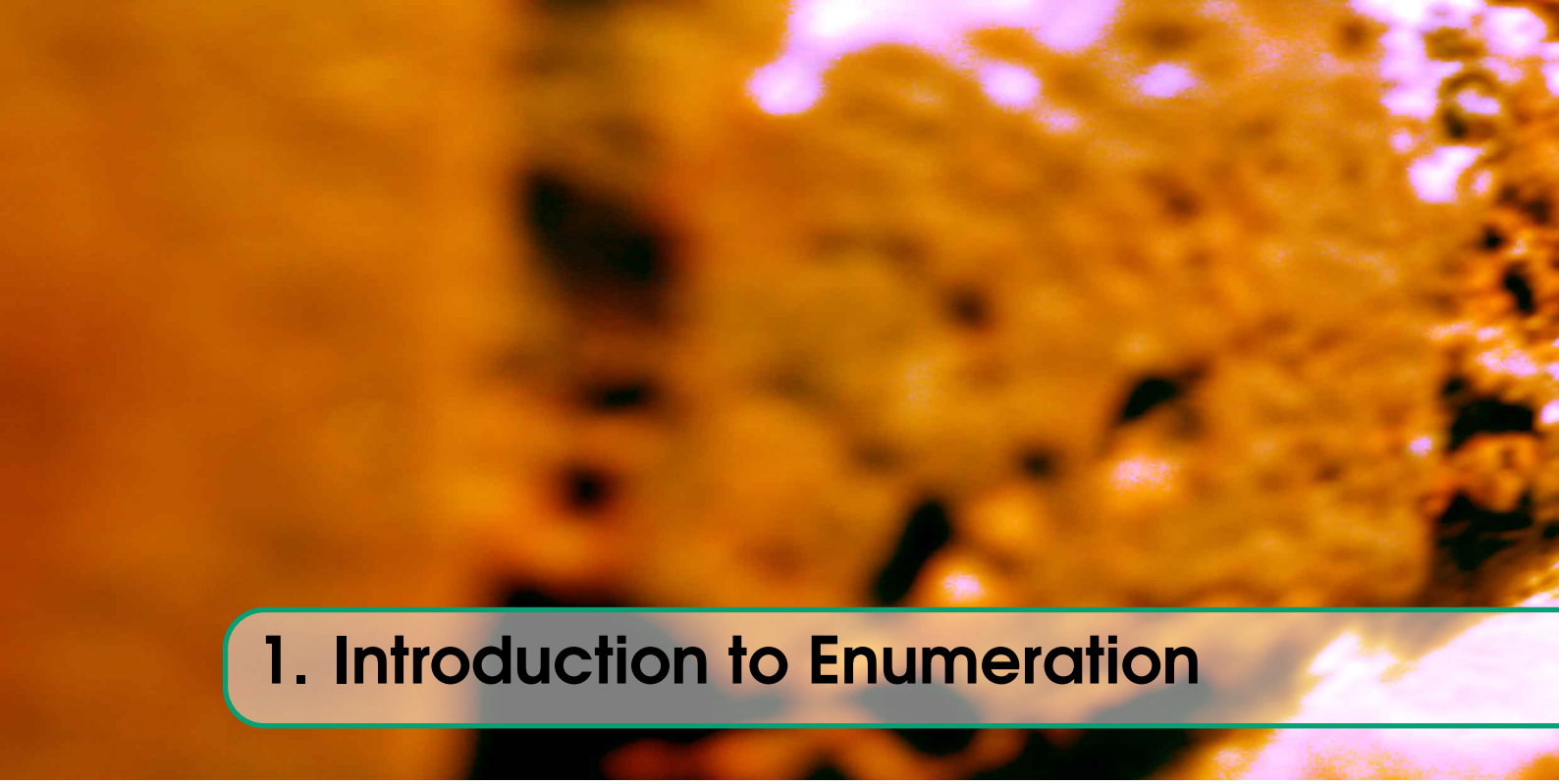
BOOK-WEBSITE.COM



*First printing, January 2016*

# Contents

# Introduction to Enumeration.



# 1. Introduction to Enumeration

# 2. Basic Principles of Enumeration.

## 2.1 The Essential Ideas.

### 2.1.1 Choices – "AND" versus "OR".

In the next few pages we will often be constructing an object of some kind by repeatedly making a sequence of choices. In order to count the total number of objects we could construct we must know how many choices are available at each step, *but we must know more*: we also need to know how to combine these numbers correctly. A generally good guideline is to look for the words "AND" and "OR" in the description of the sequence of choices available. Here are a few simple examples.

■ **Example 2.1** On a table before you are 7 apples, 8 oranges, and 5 bananas.

- *Choose an apple and a banana.*
  There are 7 choices for an apple AND 5 choices for a banana: $7 \times 5 = 35$ choices in all.
- *Choose an apple or an orange.*
  There are 7 choices for an apple OR 8 choices for an orange: $7 + 8 = 15$ choices in all.
- *Choose an apple and either an orange or a banana.*
  There are $7 \times (8 + 5) = 91$ possible choices.
- *Choose either an apple and an orange, or a banana.*
  There are $(7 \times 8) + 5 = 61$ possible choices.

■

Generally, "AND" corresponds to multiplication and "OR" corresponds to addition. The last two of the above examples show that it is important to determine exactly how the words "AND" and "OR" combine in the description of the problem.

From a mathematical point of view, "AND" corresponds to the Cartesian product of sets. If you choose one element of the set $A$ AND you choose one element of the set $B$,

then this is equivalent to choosing one element of the *Cartesian product of A and B*:

$$A \times B = \{(a,b) : \ a \in A \text{ and } b \in B\},$$

which is the set of all ordered pairs of elements $(a,b)$ with $a \in A$ and $b \in B$. In general, the cardinalities of these sets are related by the formula

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

Similarly, from a mathematical point of view, "OR" corresponds to the union of sets. If you choose one element of the set $A$ OR you choose one element of the set $B$, then this is equivalent to choosing one element of the *union of A and B*:

$$A \cup B = \{c : \ c \in A \text{ or } c \in B\},$$

which is the set of all elements $c$ which are either in $A$ or in $B$.

It is not always true that $|A \cup B| = |A| + |B|$, because any elements in both $A$ and $B$ would be counted twice by $|A| + |B|$. The *intersection of A and B* is the set

$$A \cap B = \{c : \ c \in A \text{ and } c \in B\},$$

which is the set of all elements $c$ which are both in $A$ and in $B$. What is generally true is that

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

(This is the first instance of the Principle of Inclusion/Exclusion, which will be discussed in general later on.) In particular, if $A \cap B = \varnothing$ then $|A \cup B| = |A| + |B|$. Thus, in order to interpret "OR" as addition, it is important to check that the sets of choices $A$ and $B$ have no elements in common. Such a union of sets $A$ and $B$ for which $A \cap B = \varnothing$ is called a *disjoint union* of sets.

When solving enumeration problems it is usually very useful to describe a choice sequence for constructing the set of objects of interest, paying close attention to the words "AND" and "OR".

### 2.1.2 Lists and Permutations.

A *list* of a set $S$ is a list of the elements of $S$ exactly once each, in some order. For example, the lists of the set $\{1,a,X,g\}$ are:

| | | | |
|---|---|---|---|
| $1aXg$ | $a1Xg$ | $X1ag$ | $g1aX$ |
| $1agX$ | $a1gX$ | $X1ga$ | $g1Xa$ |
| $1Xag$ | $aX1g$ | $Xa1g$ | $ga1X$ |
| $1Xga$ | $aXg1$ | $Xag1$ | $gaX1$ |
| $1gaX$ | $ag1X$ | $Xg1a$ | $gX1a$ |
| $1gXa$ | $agX1$ | $Xga1$ | $gXa1$ |

A *permutation* is a list of the set $\{1,2,...,n\}$ for some $n \in \mathbb{N}$. A permutation $\sigma : \ a_1a_2...a_n$ can be interpreted as a function $\sigma : \{1,2,...,n\} \to \{1,2,...,n\}$ by putting $\sigma(i) = a_i$ for all $1 \leq i \leq n$.

To construct a list of $S$ we can choose any element $v$ of $S$ to be the first element in the list and follow this with any list of the set $S \setminus \{v\}$. That is how the table above is arranged – each of the four columns corresponds to one choice of an element of $\{1, a, X, g\}$ to be the first element of the list. Within each column, all the lists of the remaining elements appear after the first element.

Let $p_n$ denote the number of lists of an $n$–element set $S$. The first sentence of the previous paragraph is translated into the equation

$$p_n = n \cdot p_{n-1},$$

provided that $n$ is positive. (In this equation there are $n$ choices for the first element $v$ of the list, AND $p_{n-1}$ choices for the list of $S \setminus \{v\}$ which follows it.) It is important to note here that each list of $S$ will be produced exactly once by this construction.

Since it is easy to see that $p_1 = 1$ (and $p_2 = 2$), a simple proof by induction on $n$ shows the following:

**Theorem 2.1.1** For every $n \geq 1$, the number of lists of an $n$–element set $S$ is

$$n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1.$$

In particular, taking $S = \{1, 2, ..., n\}$, this is the number of permutations of size $n$.

The term *n factorial* is used for the number $n(n-1)\cdots 3 \cdot 2 \cdot 1$, and it is denoted by $n!$ for convenience.

We also define 0! to be the number of lists of the 0–element (empty) set $\varnothing$. Since we want the equation $p_n = n \cdot p_{n-1}$ to hold when $n = 1$, and since $p_1 = 1! = 1$, we conclude that $0! = p_0 = 1$ as well.

### 2.1.3 Subsets.

A *subset* of a set $S$ is a collection of some (perhaps none or all) of the elements of $S$, at most once each and in no particular order.

To specify a particular subset $A$ of $S$, one has to decide for each element $v$ of $S$ whether $v$ is in $A$ or $v$ is not in $A$. Thus we have two choices – $v \in A$ OR $v \notin A$ – for each element $v$ of $S$. If $S = \{v_1, v_2, ..., v_n\}$ has $n$ elements then the total number of choices is $2^n$ since we have 2 choices for $v_1$ AND 2 choices for $v_2$ AND ... AND 2 choices for $v_n$. Therefore....

**Theorem 2.1.2** For every $n \geq 0$, the number of subsets of an $n$–element set is $2^n$.

### 2.1.4 Partial lists.

A *partial list* of a set $S$ is a list of a subset of $S$. That is, it is a list of some (perhaps none or all) of the elements of $S$, at most once each and listed in some particular order. We are going to count partial lists of length $k$ of an $n$–element set.

First think about the particular case $n = 6$ and $k = 3$, and the set $S = \{a, b, c, d, e, f\}$. A partial list of $S$ of length 3 is a list $xyz$ of elements of $S$, which must all be different. There are:

6 choices for $x$ (since $x$ is in $S$), AND

5 choices for $y$ (since $y \in S$ but $y \neq x$), AND

4 choices for $z$ (since $z \in S$ but $z \neq x$ and $z \neq y$).
Altogether there are $6 \cdot 5 \cdot 4 = 120$ partial lists of $\{a,b,c,d,e,f\}$ of length 3.

This kind of reasoning works just as well in the general case. If $S$ is an $n$–element set and we want to construct a partial list $v_1 v_2 ... v_k$ of elements of $S$ of length $k$, then there are:
$n$ choices for $v_1$, AND
$n-1$ choices for $v_2$, AND
....
$n-(k-2)$ choices for $v_{k-1}$, AND
$n-(k-1)$ choices for $v_k$.

This proves the following result.

**Theorem 2.1.3** For $n,k \geq 0$, the number of partial lists of length $k$ of an $n$–element set is $n(n-1)\cdots(n-k+2)(n-k+1)$.

Notice that if $k > n$ then the number 0 will appear as one of the factors in the product $n(n-1)\cdots(n-k+2)(n-k+1)$. This makes sense, because if $k > n$ then there are no partial lists of length $k$ of an $n$–element set. On the other hand, if $0 \leq k \leq n$ then we could also write this product as

$$n(n-1)\cdots(n-k+2)(n-k+1) = \frac{n!}{(n-k)!}.$$

### 2.1.5 $k$-element Subsets.

We refine the result of Section 3 by counting subsets of an $n$–element set $S$ which have a particular size $k$. So for $n,k \geq 0$ let $\binom{n}{k}$ denote the number of $k$–element subsets of an $n$–element set $S$. Notice that if $k < 0$ or $k > n$ then $\binom{n}{k} = 0$ because in these cases it is impossible for $S$ to have a $k$–element subset. Thus we need only consider $k$ in the range $0 \leq k \leq n$.

To count $k$–element subsets of $S$ we consider another way of constructing a partial list of length $k$ of $S$. Specifically, we can choose a $k$–element subset $A$ of $S$ AND a list of $A$. The result will be a list of a subset of $S$ of length $k$. Since every partial list of length $k$ of $S$ is constructed exactly once in this way, this translates into the equation

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

In summary, we have proved the following result.

**Theorem 2.1.4** For $0 \leq k \leq n$, the number of $k$–element subsets of an $n$–element set is

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

The numbers $\binom{n}{k}$ are read as "$n$ choose $k$" and are called *binomial coefficients*.

### 2.1.6 Think of What the Numbers Mean.

Usually, when faced with a formula to prove, one's first thought is to prove it by algebraic calculations, or perhaps with an induction argument, or maybe with a combination of the

two. But often that is not the easiest way, nor is it the most informative. A much better strategy is one which gives some insight into the meaning of all of the parts of the formula. If we can interpret all the numbers as counting things, addition as "OR", and multiplication as "AND", then we can hope to find an explanation of the formula by constructing some objects in the correct way.

■ **Example 2.2** Consider the equation, for any $n \geq 0$:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

This could be proved by induction on $n$, but many more details would have to be given and the proof would not address the true "meaning" of the formula. Instead, let's interpret everything combinatorially:

- $2^n$ is the number of subsets of an $n$–element set, $\{1,2,...,n\}$ say;
- $\binom{n}{k}$ is the number of $k$–element subsets of $\{1,2,...,n\}$, for each $0 \leq k \leq n$;
- addition corresponds to "OR" (that is, disjoint union of sets).

So, this formula is saying that choosing a subset of $\{1,2,...,n\}$ (in one of $2^n$ ways) is equivalent to choosing a $k$–element subset of $\{1,2,...,n\}$ (in one of $\binom{n}{k}$ ways) for exactly one value of $k$ in the range $0 \leq k \leq n$. Said that way the formula becomes self–evident, and there is nothing more to prove. ■

■ **Example 2.3** Consider the equation

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

where we are using the fact that $\binom{m}{j} = 0$ if $j < 0$ or $j > m$. This equation can be proven algebraically from the formula of Theorem 2.1.4, and that is a good exercise which I encourage you to try. But a more informative proof interprets these numbers combinatorially as follows:

- $\binom{n}{k}$ is the number of $k$–element subsets of $\{1,2,...,n\}$;
- $\binom{n-1}{k-1}$ is the number of $(k-1)$–element subsets of $\{1,2,...,n-1\}$;
- $\binom{n-1}{k}$ is the number of $k$–element subsets of $\{1,2,...,n-1\}$;
- addition corresponds to disjoint union of sets.

So, this equation is saying that choosing a $k$–element subset $A$ of $\{1,2,...,n\}$ is equivalent to either choosing a $(k-1)$–element subset of $\{1,2,...,n-1\}$ or a $k$–element subset of $\{1,2,...,n-1\}$. This is perhaps not as clear as the previous example, but the two cases depend upon whether the chosen $k$–element subset $A$ of $\{1,2,...,n\}$ is such that $n \in A$ OR $n \notin A$. If $n \in A$ then $A \setminus \{n\}$ is a $(k-1)$–element subset of $\{1,2,...,n-1\}$, while if $n \notin A$ then $A$ is a $k$–element subset of $\{1,2,...,n-1\}$. This construction explains the correspondence, proving the formula. ■

This principle – interpreting equations combinatorially and proving the formulas by describing explicit correspondences between sets of objects – is one of the most important and powerful ideas in enumeration. We'll have a lot of practice using this way of thinking in the next few weeks.

Incidentally, the equation in the Example 2.3 is a very useful recurrence relation for

computing binomial coefficients quickly. Together with the facts

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

and $\binom{n}{0} = \binom{n}{n} = 1$ it can be used to grind out any number of binomial coefficients without difficulty. The resulting table is known as *Pascal's Triangle*:

| $n\backslash k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 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 | | |
| 7 | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 | |
| 8 | 1 | 8 | 28 | 56 | 70 | 56 | 28 | 8 | 1 |

### 2.1.7 Multisets.

Imagine a bag which contains a large number of marbles of three colours – red, green, and blue, say. The marbles are all indistinguishable from one another except for their colours. There are $N$ marbles of each colour, where $N$ is very, very large (more precisely we should be considering the limit as $N \to \infty$). If I reach into the bag and pull out a handful of 11 marbles, I will have $r$ red marbles, $g$ green marbles, and $b$ blue marbles, for some nonnegative integers $(r,g,b)$ such that $r+g+b = 11$. How many possibile outcomes are there?

The word "multiset" is meant to suggest a set in which the objects can occur more than once. For example, the outcome $(4,5,2)$ in the above situation corresponds to the "set" $\{R,R,R,R,G,G,G,G,G,B,B\}$ in which $R$ is a red marble, $G$ is a green marble, and $B$ is a blue marble. This is an 11–element multiset with elements of three types. The number of these multisets is the solution to the above problem.

In general, if there are $t$ types of element then a *multiset of size $n$ with elements of $t$ types* is a sequence of nonnegative integers $(m_1,\ldots,m_t)$ such that

$$m_1 + m_2 + \cdots + m_t = n.$$

The interpretation is that $m_i$ is the number of elements of the multiset which are of the $i$–th type, for each $1 \le i \le t$.

**Theorem 2.1.5** For any $n \ge 0$ and $t \ge 1$, the number of $n$–element multisets with elements of $t$ types is

$$\binom{n+t-1}{t-1}.$$

*Proof.* Think of what that number means! By Theorem 2.1.4, $\binom{n+t-1}{t-1}$ is the number of $(t-1)$–element subsets of an $(n+t-1)$–element set. So, let's write down a row of

$(n+t-1)$ circles from left to right:

O O O O O O O O O O O O O

and cross out some $t-1$ of these circles to choose a $(t-1)$–element subset:

O O O O X O O O O O X O O

Now the $t-1$ crosses chop the remaining sequence of $n$ circles into $t$ segments of consecutive circles. (Some of these segments might be empty, which is to say of length zero.) Let $m_i$ be the length of the $i$–th segment of consecutive O-s in this construction. Then $m_1+m_2+\cdots+m_t=n$, so that $(m_1,m_2,...,m_t)$ is an $n$–element multiset with $t$ types. Conversely, if $(m_1,m_2,...,m_t)$ is an $n$–element multiset with $t$ types then write down a sequence of $m_1$ O-s, then an X, then $m_2$ O-s, then an X, and so on, finishing with an X and then $m_t$ O-s. The positions of the X-s will indicate a $(t-1)$–element subset of the positions $\{1,2,...,n+t-1\}$.

The construction of the above paragraph shows how to translate between $(t-1)$–element subsets of $\{1,2,...,n+t-1\}$ and $n$–element multisets with $t$ types of element. This one–to–one correspondence completes the proof of the theorem. ■

To answer the original question of this section, the number of 11–element multisets with elements of 3 types is $\binom{11+3-1}{3-1}=\binom{13}{2}=78$.

### 2.1.8 Bijective Proofs.

The arguments above, counting lists, permutations, subsets, multisets, and so on, can be phrased more formally using the idea of bijections between finite sets. In simple cases as we have seen so far this is not always necessary, but it is good style. In more complicated situations, as we will see in Chapters 3 and 5, it is a very useful way to organize one's thoughts.

**Definition 2.1.1** Let $f:\mathcal{A}\to\mathcal{B}$ be a function from a set $\mathcal{A}$ to a set $\mathcal{B}$.

- The function $f$ is *surjective* if for every $b\in\mathcal{B}$ there exists an $a\in\mathcal{A}$ such that $f(a)=b$.
- The function $f$ is *injective* if for every $a,a'\in\mathcal{A}$, if $f(a)=f(a')$, then $a=a'$.
- The function $f$ is *bijective* if it is both surjective and injective.

Functions with these properties are called surjections, injections, or bijections, respectively. An older terminology – now out of fashion – is that surjections are "onto" functions, injections are "one-to-one" functions, and bijections are "one-to-one and onto".

The point of Definition is the following. Consider a bijection $f:\mathcal{A}\to\mathcal{B}$. Then every $b\in\mathcal{B}$ is the image of at least one $a\in\mathcal{A}$, since $f$ is surjective. On the other hand, every $b\in\mathcal{B}$ is the image of at most one $a\in\mathcal{A}$, since $f$ is injective. Therefore, every $b\in\mathcal{B}$ is the image of exactly one $a\in\mathcal{A}$. In other words, the relation $f(a)=b$ pairs off all the elements of $\mathcal{A}$ with all the elements of $\mathcal{B}$. It follows that $\mathcal{A}$ and $\mathcal{B}$ have the same number of elements – that is, $|\mathcal{A}|=|\mathcal{B}|$.

**Proposition 2.1.6** Let $f:\mathcal{A}\to\mathcal{B}$ and $g:\mathcal{B}\to\mathcal{A}$ be functions between two sets $\mathcal{A}$ and $\mathcal{B}$. Assume the following.

- For all $a \in \mathcal{A}$, $g(f(a)) = a$.
- For all $b \in \mathcal{B}$, $f(g(b)) = b$.

Then both $f$ and $g$ are bijections. Moreover, for $a \in \mathcal{A}$ and $b \in \mathcal{B}$, we have $f(a) = b$ if and only if $g(b) = a$.

The proof is left as an exercise.

A pair of functions as in Proposition 2.1.6 are called *mutually inverse bijections*. The notation $g = f^{-1}$ and $f = g^{-1}$ is used to denote this relation. Notice that for a bijection $f$, we have $(f^{-1})^{-1} = f$.

Here are two examples of this way of thinking.

▪ **Example 2.4 — Subsets and indicator vectors..** Let $\mathcal{P}(n)$ be the set of all subsets of $\{1,2,...,n\}$, and let $\{0,1\}^n$ be the set of all *indicator vectors* $\alpha = (a_1, a_2, ..., a_n)$ in which each coordinate is either 0 or 1. There is a bijection between these two sets. For a subset $S \subseteq \{1,2,...,n\}$, define the vector $\alpha(S) = (a_1(S), a_2(S), ..., a_n(S))$ by saying that for each $1 \leq i \leq n$,

$$a_i(S) = \begin{cases} 1 & \text{if } i \in S, \\ 0 & \text{if } i \notin S. \end{cases}$$

Conversely, for an indicator vector $\alpha = (a_1, ..., a_n)$ define a subset $S(\alpha)$ by saying that

$$S(\alpha) = \{i \in \{1,2,...,n\} : \ a_i = 1\}.$$

For example, when $n = 8$ the subset $\{2,3,5,7\}$ corresponds to the indicator vector $(0,1,1,0,1,0,1,0)$. The constructions $S \mapsto \alpha(S)$ and $\alpha \mapsto S(\alpha)$ are mutually inverse bijections between the sets $\mathcal{P}(n)$ and $\{0,1\}^n$ as in Proposition 2.1.6. It follows that $|\mathcal{P}(n)| = |\{0,1\}^n| = 2^n$. This is a formalization of the argument in subsection 2.1.3. ▪

▪ **Example 2.5 — Subsets and multisets..** Let $\mathcal{M}(n,t)$ be the set of all multisets of size $n$ with $t$ types of elements. We saw in Theorem 2.1.5 that $|\mathcal{M}(n,t)| = \binom{n+t-1}{t-1}$. In fact, the proof of Theorem 2.1.5 is essentially a bijection between the set $\mathcal{M}(n,t)$ and the set $\mathcal{B}(n+t-1,t-1)$ of all $(t-1)$-element subsets of the set $\{1,2,...,n+t-1\}$. The fact that $|\mathcal{B}(n+t-1,t-1)| = \binom{n+t-1}{t-1}$ follows from Theorem 2.1.4. Here is a more precise description of this bijection.

Let $S$ be any $(t-1)$-element subset of $\{1,2,...,n+t-1\}$. We can sort the elements of $S$ in increasing order: $S = \{s_1, s_2, ..., s_{t-1}\}$ in which $s_1 < s_2 < \cdots < s_{t-1}$. For notational convenience, let $s_0 = 0$ and let $s_t = n+t$. Now define a sequence $\mu = (m_1, m_2, ..., m_t)$ by letting $m_i = s_i - s_{i-1} - 1$ for all $1 \leq i \leq t$.

For example, with $n = 10$ and $t = 4$, consider the 3-element subset $S = \{2,7,11\}$ of $\{1,2,...,13\}$. Then $s_0 < s_1 < \cdots < s_t$ is $0 < 2 < 7 < 11 < 14$, the sequence of differences is $(2,5,4,3)$, and subtracting 1 from each of these yields $\mu = (1,4,3,2)$. Notice that $\mu$ is a multiset of size 10 with 4 types of elements.

In general, since $s_{i-1} < s_i$ for all $1 \leq i \leq t$, it follows that $m_i = s_i - s_{i-1} - 1$ is a nonnegative integer. Also, since $s_t = n+t$, it follows that $m_1 + m_2 + \cdots + m_t = s_t - t = n$. That is, $\mu$ is a multiset of size $n$ with elements of $t$ types. This describes a function $S \mapsto \mu$ from the set $\mathcal{B}(n+t-1,t-1)$ to the set $\mathcal{M}(n,t)$. This is in fact a bijection between these two sets.

To show that our construction $S \mapsto \mu$ is a bijection, we will describe its inverse function. Begin with a multiset $\mu = (m_1, m_2, ..., m_t)$ of size $n$ with $t$ types of elements. For each

$1 \leq i \leq t-1$, let $s_i = m_1 + m_2 + \cdots + m_i + i$. Notice that

$$1 \leq s_1 < s_2 < \cdots < s_{t-1} \leq n+t-1.$$

Therefore, $S = \{s_1, s_2, ..., s_{t-1}\}$ is a $(t-1)$-element subset of $\{1, 2, ..., n+t-1\}$.

To finish this example, one must check that these constructions, $S \mapsto \mu$ and $\mu \mapsto S$, are mutually inverse bijections as in Proposition 2.1.6. This is left as an exercise. ∎

### 2.1.9 The Principle of Inclusion/Exclusion.

In a vase is a bouquet of flowers. Each flower is (at least one of) fresh, fragrant, or colourful:
(a) 11 flowers are fresh;
(b) 7 flowers are fragrant;
(c) 8 flowers are colourful;
(d) 6 flowers are fresh and fragrant;
(e) 5 flowers are fresh and colourful;
(f) 2 flowers are fragrant and colourful;
(g) 2 flowers are fresh, fragrant, and colourful.
How many flowers are in the bouquet?

The Principle of Inclusion/Exclusion is a systematic method for answering such questions, which involve overlapping conditions which can be satisfied (or not) in various combinations.

For a small problem like the one above we can work backwards as follows:
(h) from (g) and (f) there are 0 flowers which are fragrant and colourful but not fresh;
(i) from (g) and (e) there are 3 flowers which are fresh and colourful but not fragrant;
(j) from (g) and (d) there are 4 flowers which are fresh and fragrant but not colourful;
(k) from (c)(g)(h)(i) there are 3 flowers which are colourful but neither fresh not fragrant;
($\ell$) from (b)(g)(h)(j) there is 1 flower which is fragrant but neither fresh nor colourful;
(m) from (a)(g)(i)(j) there are 2 flowers which are fresh but neither fragrant nor colourful.
The total number of flowers is counted by the disjoint union of the cases (g) through (m); that is $2+0+3+4+3+1+2 = 15$.

A *Venn diagram* is extremely useful for organizing this calculation. Figure 1 is a Venn diagram for the three sets involved in this question. Item (g) in the original data gives the number of flowers (2) counted in the central triangle. The subsequent steps (h) to (m) calculate the rest of the numbers in the diagram, moving outwards from the center.

The above works very well for three properties (fresh, fragrant, colourful) but becomes increasingly difficult to apply as the number of properties increases. Consider this alternative formula:

$$(a)+(b)+(c)-(d)-(e)-(f)+(g) = 11+7+8-6-5-2+2 = 15.$$

This looks much easier to apply, and it gives the right answer, always. Why? That is the Principle of Inclusion/Exclusion, which we now explain in general.

Let $A_1$, $A_2$,... $A_m$ be finite sets. We want a formula for the cardinality of the union of these sets $A_1 \cup A_2 \cup \cdots \cup A_m$. First a bit of notation: if $S$ is a nonempty subset of $\{1, 2, ..., m\}$ then let $A_S$ denote the intersection of the sets $A_i$ for all $i \in S$. So, for example, with this notation we have $A_{\{2,3,5\}} = A_2 \cap A_3 \cap A_5$.

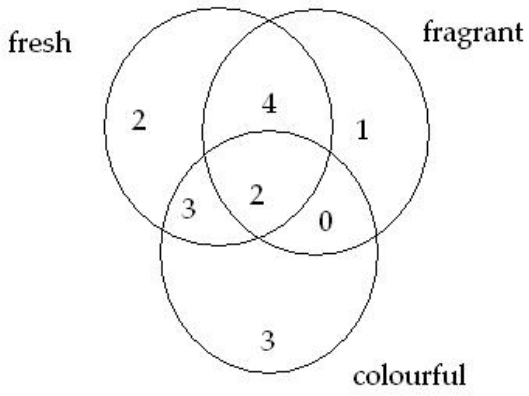



Figure 2.1: A Venn diagram for three sets.

**Theorem 2.1.7 — Inclusion/Exclusion.** Let $A_1, A_2, ..., A_m$ be finite sets. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{\varnothing \neq S \subseteq \{1,2,...,m\}} (-1)^{|S|-1} |A_S|.$$

(In this formula the summation is over all nonempty subsets of $\{1,2,..,m\}$.)

We prove Theorem 2.1.7 in Section 3.4, but all that is required is the Binomial Theorem 3.1.1.

### 2.1.10 Combinatorial Probabilities.

We can reinterpret counting problems in terms of probabilities by making one additional hypothesis. That hypothesis is that **every possible outcome is equally likely**. The exact definition of what is an "outcome" depends on the particular problem. If $\Omega$ denotes a finite set of all possible outcomes, then any subset $E$ of $\Omega$ is what a probabilist calls an *event*. The probability that a randomly chosen outcome from $\Omega$ is in the set $E$ is $|E|/|\Omega|$ exactly because every outcome has likelyhood $1/|\Omega|$ of being chosen, and there are $|E|$ elements in $E$. Here are a few examples to illustrate these ideas.

■ **Example 2.6** *What is the probability that a random subset of* $\{1,2,...,8\}$ *has at most* 3 *elements?*
Here an outcome is a subset of $\{1,2,...,8\}$, and there are $2^8 = 256$ such subsets. The number of subsets of $\{1,2,...,8\}$ with at most 3 elements is

$$\binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} = 1 + 8 + 28 + 56 = 93.$$

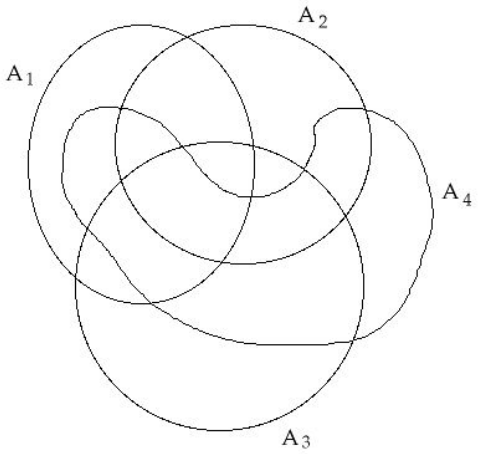



Figure 2.2: A Venn diagram for four sets.

So the probability in question is

$$\frac{93}{256} = 0.363281...$$

to six decimal places. ∎

∎ **Example 2.7** *What is the probability that a random list of the set* $\{a,b,c,d,e,f\}$ *contains the letters* $fad$ *as a consecutive subsequence?*
Here an outcome is a list of $\{a,b,c,d,e,f\}$, and there are $6! = 720$ such lists. Those lists of this set which contain $fad$ as a consecutive subsequence can be constructed uniquely as the lists of the set $\{b,c,e,fad\}$, so there are $4! = 24$ of these. Thus, the probability in question is

$$\frac{24}{720} = \frac{1}{30} = 0.03333...$$

∎

∎ **Example 2.8** *What is the probability that a randomly chosen* 2*–element multiset with* $t$ *types of element has both elements of the same type?*
The outcomes are the 2–element multisets with $t$ types, numbering

$$\binom{2+t-1}{t-1} = \binom{t+1}{t-1} = \binom{t+1}{2} = \frac{(t+1)t}{2}$$

in total. Of these, exactly $t$ of them have both elements of the same type – choose one of the $t$ types and take two elements of that type. Thus, the probability in question is

$$\frac{2t}{(t+1)t} = \frac{2}{t+1}.$$

The values for the first few $t$ are given in the following table to four decimal places:

| $t$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| | 1.0000 | 0.6667 | 0.5000 | 0.4000 | 0.3333 | 0.2857 | 0.2500 |

■

## 2.2 Examples and Applications.

In this section we consider a few more substantial applications of these ideas.

### 2.2.1 The Vandermonde Convolution Formula.

For natural numbers $m$, $n$, and $k$:

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}.$$

For example, with $m = 4$ and $n = 2$ and $k = 3$ this says that

$$\binom{6}{3} = \binom{4}{0}\binom{2}{3} + \binom{4}{1}\binom{2}{2} + \binom{4}{2}\binom{2}{1} + \binom{4}{3}\binom{2}{0}.$$

(Of course, $\binom{2}{3} = 0$, but that doesn't matter.)

In general, this can be proven algebraically by induction on $m+n$ but the proof is detailed and doesn't give much insight into what the formula "means". (The formula can also be deduced easily from the Binomial Theorem, as we shall see in 3.1.)

Here is a direct **combinatorial** proof, illustrating the strategy of thinking about what the numbers mean. On the LHS, $\binom{m+n}{k}$ is the number of $k$–element subsets $S$ of the set $\{1,2,...,m+n\}$. On the RHS, the number can be produced as follows:

- choose a value of $j$ in the range $0 \le j \le k$, and
- choose a $j$–element subset $A$ of $\{1,2,...,m\}$, and
- choose a $(k-j)$–element subset of $\{m+1,...,m+n\}$. (Notice that the set $\{m+1,...,m+n\}$ has $n$ elements, so it has $\binom{n}{k-j}$ subsets of size $k-j$.)

Now the formula is proved by describing a bijection between the $k$–element subsets $S$ of $\{1,2,...,m+n\}$ counted on the LHS, and the pairs $(A,B)$ of subsets counted on the RHS. This correspondence is easy to describe: given a $k$–element subset $S$ of $\{1,2,...,m+n\}$ we let

$$A = S \cap \{1,2,...,m\}$$

and

$$B = S \cap \{m+1, m+2, ..., m+n\}.$$

Conversely, given a pair of subsets $(A,B)$ satisfying the conditions on the RHS of the formula, we let $S = A \cup B$. After some thought you'll see that these constructions $S \mapsto (A,B)$ and $(A,B) \mapsto S$ are mutually inverse bijections. Therefore, there are the same number of objects on each side, and the formula is proved.

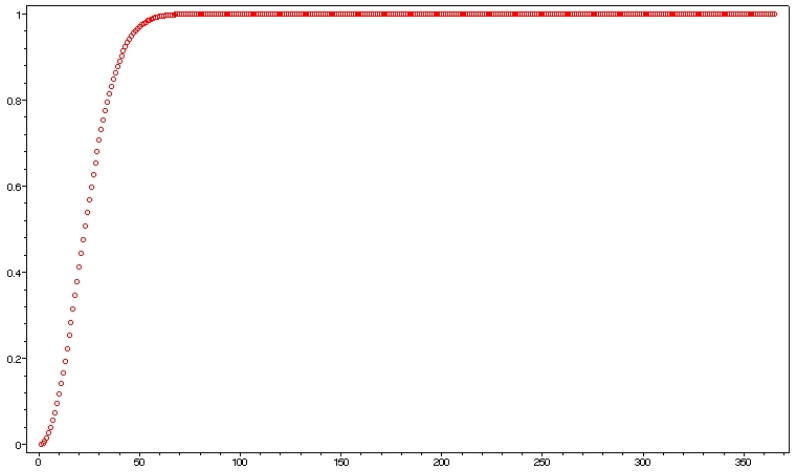



Figure 2.3: The probability of a common birthday among $n$ random people

### 2.2.2 Common Birthdays.

Let $p(n)$ denote the probability that in a randomly chosen group of $n$ people, at least two of them are born on the same day of the year. What does the function $p(n)$ look like?

To simplify the analysis, we will ignore the existence of leap years and assume that every year has exactly 365 days. (This introduces a tiny error but does not change the qualitative "shape" of the answer.) Moreover, we will also assume that people's birthdays are independently and uniformly distributed over the 365 days of the year, so that we can use the ideas of combinatorial probability theory. (This is a reasonable approximation, since twins are relatively rare.)

To begin with, $p(1) = 0$ since there is only $n = 1$ person in the group. Also, if $n > 365$ then $p(n) = 1$ since there are more people in the group than days in a year, so at least two people in the group must have the same birthday.

For $n$ in the range $2 \leq n \leq 365$ it is quite complicated to analyze the probability $p(n)$ directly. However, the complementary probability $1 - p(n)$ is relatively easy to compute. From the definition of $p(n)$ we see that $1 - p(n)$ is the probability that in a randomly chosen group of $n$ people, **no two of them** are born on the same day of the year. This model is equivalent to rolling "no pair" when throwing $n$ independent dice each with 365 sides. If we list the people in the group as $P_1$, $P_2$,..., $P_n$ in any arbitrary order, then their birthdays must form a partial list of the 365 days of the year, of length $n$. There are $365!/(365-n)!$ such partial lists. Since the total number of outcomes is $365^n$, we have derived the formula

$$1 - p(n) = \frac{365!}{(365-n)!365^n}.$$

Therefore

$$p(n) = 1 - \frac{365!}{(365-n)!365^n}.$$

To give you some feeling for what this probability looks like, here is a table of $p(n)$ (rounded to six decimal places) for selected values of $2 \leq n \leq 365$. Figure 2.3 gives a graph of this function.

| $n$ | $p(n)$ | $n$ | $p(n)$ | $n$ | $p(n)$ |
|---|---|---|---|---|---|
| 2 | 0.002740 | 25 | 0.568700 | 70 | 0.999160 |
| 3 | 0.008204 | 30 | 0.706316 | 80 | 0.999914 |
| 4 | 0.016356 | 35 | 0.814383 | 100 | 1. |
| 5 | 0.027136 | 40 | 0.891232 | 150 | 1. |
| 10 | 0.116948 | 45 | 0.940976 | 200 | 1. |
| 15 | 0.252901 | 50 | 0.970374 | 250 | 1. |
| 20 | 0.411438 | 60 | 0.994123 | 300 | 1. |

It is a rather surprising fact that $p(23) = 0.507297$ – so that if you randomly choose a set of 23 people on earth then there is a slightly better than 50% chance that at least two of them will have the same birthday. (Approximately – we have ignored leap years and twins.)

### 2.2.3 An Example with Multisets.

A packet of *Maynard's Wine Gums* consists of a roll or packet of 10 candies, each of which has one of five "flavours" – *Green, Yellow, Orange, Red*, or *Purple*. I especially like the purple ones. What is the chance that when I buy a packet of Wine Gums I get exactly $k$ purple candies (for each $0 \leq k \leq 10$)?

This example is designed to illustrate the fact that the probabilities depend on which model is used to analyze the situation. There are two reasonable possibilities for this problem, which I will call the **dice model** and the **multiset model**.

In the "dice model" we keep track of the fact that the candies are stacked up in the roll from bottom to top, so there is a natural sequence $(c_1, c_2, ...., c_{10})$ of flavours one sees when the packet is opened. For example, the sequences

$$(G,P,R,Y,Y,G,O,R,Y,O)$$

and

$$(Y,G,O,P,R,R,Y,G,O,Y)$$

count as different outcomes in this model. We have a sequence of 10 candies, and a choice of one of 5 flavours for each candy, giving a total of $5^{10} = 9765625$ outcomes. (This is equivalent to rolling a sequence of ten 5–sided dice, hence the name for the model.)

In the "multiset model" we disregard the order in which the candies occur in the packet as being an inessential detail. The only important information about the packet is the number of candies of each type that it contains. For example, both of the outcomes in the previous paragraph reduce to the same multiset

$$\{G,G,Y,Y,Y,O,O,R,R,P\}$$

or $(2,3,2,2,1)$ in this model. Thus we are regarding the packet as a multiset of size 10 with 5 types of element, giving a total of $\binom{10+5-1}{5-1} = \binom{14}{4} = 1001$ outcomes.

Notice that the number of outcomes in the dice model is much larger than in the multiset model. It should come as no surprise, then, that the probabilities we compute will depend strongly on which of these two models we consider. (The *true values* for the probabilities depend on the details of the manufacturing process by which the rolls or packets are made. These cannot be calculated, but must be measured instead.)

Let us consider the dice model first, and let $d(k)$ denote the probability of getting exactly $k$ purple candies in a packet. There are $\binom{10}{k}$ choices for the positions of these $k$ purple candies, and $(5-1)^{10-k}$ choices for the sequence of (non–purple) flavours of the other $10-k$ candies. This gives a total of $\binom{10}{k}4^{10-k}$ outcomes with exactly $k$ purple candies in this model. Therefore,

$$d(k) = \binom{10}{k}\frac{4^{10-k}}{5^{10}}$$

for each $0 \le k \le 10$. Here is a table of these probabilities (rounded to six decimal places).

| $k$ | $d(k)$ | $k$ | $d(k)$ |
|---|---|---|---|
| 0 | 0.107374 | | |
| 1 | 0.268435 | 6 | 0.005505 |
| 2 | 0.301990 | 7 | 0.000786 |
| 3 | 0.201327 | 8 | 0.000074 |
| 4 | 0.088080 | 9 | 0.000004 |
| 5 | 0.026424 | 10 | 0.000000 |

Next let's consider the multiset model, and let $m(k)$ denote the probability of getting exactly $k$ purple candies in a packet. If we have $k$ purple candies then the rest of the candies form a multiset of size $10-k$ with elements of 4 types, so there are $\binom{10-k+4-1}{4-1} = \binom{13-k}{3}$ such outcomes in this model. Therefore,

$$m(k) = \frac{\binom{13-k}{3}}{\binom{14}{4}}$$

for each $0 \le k \le 10$. Here is a table of these probabilities (rounded to six decimal places).

| $k$ | $m(k)$ | $k$ | $m(k)$ |
|---|---|---|---|
| 0 | 0.285714 | | |
| 1 | 0.219780 | 6 | 0.034965 |
| 2 | 0.164835 | 7 | 0.019980 |
| 3 | 0.119880 | 8 | 0.009990 |
| 4 | 0.083916 | 9 | 0.003996 |
| 5 | 0.055944 | 10 | 0.000999 |

The differences between the two models are clearly seen in these tables.

In closing, here are two more points about these models.

First, given a multiset $(m_1,\ldots,m_t)$ of size $n$ with elements of $t$ types, the number of outcomes in the dice model which "reduce" to this multiset is

$$\binom{n}{m_1,\ldots,m_t} = \frac{n!}{m_1!\cdot m_2!\cdots m_t!},$$

called a *multinomial coefficient*. This can be seen intuitively by arranging the $n$ elements of the multiset in a line in one of $n!$ ways, and noticing that since we can't tell the $m_i$ elements of type $i$ apart we can freely rearrange them in $m_i!$ ways without changing the

arrangement. (A more careful argument goes by induction on $t$ using the case $t = 2$ of binomial coefficients.)

For the second point, the above analysis of the multiset model can be generalized to prove the following identity: for any integers $n \geq 1$ and $t \geq 2$:

$$\binom{n+t-1}{t-1} = \sum_{k=0}^{n} \binom{n-k+t-2}{t-2}.$$

(This is a good exercise – think about what the numbers mean!)

### 2.2.4 Poker Hands.

Poker is played with a standard deck of 52 cards, divided into four *suits* (Spades ♠, Hearts ♡, Diamonds ♢, and Clubs ♣) with 13 cards in each suit:
A (Ace), 2, 3, 4, 5, 6, 7, 8, 9, 10, J (Jack), Q (Queen), K (King).
An Ace can be *high* (above K) or *low* (below 2) at the player's choice. Many variations on the game exist, but the common theme is to make the best 5–card hand according to the ranking of poker hands. This ranking is determined by how unlikely it is to be dealt such a hand. The types of hand are as follows:

- Straight Flush: this is five cards of the same suit with consecutive values.
  For example, 8♡ 9♡ 10♡ $J$♡ $Q$♡.
- Four of a Kind (or Quads): this is four cards of the same value, with any fifth card.
  For example, 7♠ 7♡ 7♢ 7♣ 4♢.
- Full House (or Tight, or Boat): this is three cards of the same value, and a pair of cards of another value.
  For example, 9♠ 9♡ 9♢ $A$♢ $A$♣.
- Flush: this is five cards of the same suit, but not with consecutive values.
  For example, 3♡ 7♡ 10♡ $J$♡ $K$♡.
- Straight: this is five cards with consecutive values, but not of the same suit.
  For example, 8♡ 9♣ 10♠ $J$♡ $Q$♢.
- • Three of a Kind (or Trips): this is three cards of the same value, and two more cards not of the same value.
  For example, 8♠ 8♡ 8♢ $K$♢ 5♣.
- Two Pair: this is self–explanatory.
  For example, $J$♡ $J$♣ 6♢ 6♣ $A$♠.
- One Pair: this is also self–explanatory.
  For example, $Q$♠ $Q$♢ 8♢ 7♣ 2♠.
- Busted Hand: this is anything not covered above.
  For example, $K$♠ $Q$♢ 8♢ 7♣ 2♠.

Of course, there are $\binom{52}{5} = 2598960$ possible 5–element subsets of a standard deck of 52 cards, so this is the total number of possible poker hands. How many of these hands are of each of the above types? The answers are easily availabe on the WWWeb, so there's no sense trying to keep them secret. Here they are: $N$ is the number of outcomes of each type, and $p = N/\binom{52}{5}$ is the probability of each type of outcome.

| Hand | $N$ | $p$ |
|---|---|---|
| Straight Flush | 40 | 0.000015 |
| Quads | 624 | 0.000240 |
| Full House | 3744 | 0.001441 |
| Flush | 5108 | 0.001965 |
| Straight | 10200 | 0.003925 |
| Trips | 54912 | 0.021128 |
| Two Pair | 123552 | 0.047539 |
| One Pair | 1098240 | 0.422569 |
| Busted | 1302540 | 0.501177 |

The derivation of these numbers is an excellent exercise, so we will do only two of the cases – Straight, and Busted – as illustrations.

To construct a Straight hand there are 10 choices for the consecutive ranks of the cards ($A2345$, 23456, ... up to $10JQKA$), and $4^5$ choices for the suits on the cards. However, four of these choices for suits give all five cards the same suit – these lead to straight flushes and must be discounted. Hence the total number of straights is $10 \cdot [4^5 - 4] = 10200$.

To construct a Busted hand there are $\binom{13}{5} - 10$ choices for 5 values of cards which are not consecutive (no straight) and have no pairs. Having chosen these values there are $4^5 - 4$ choices for the suits on the cards which do not give all five cards the same suit (no flush). Hence the total number of busted hands is $[\binom{13}{5} - 10] \cdot [4^5 - 4] = 1302540$.

The remaining cases are left as exercises.

### 2.2.5 Derangements.

A group of eight people meet for dinner at a fancy restaurant and check their coats at the door. After a delicious gourmet meal the group leaves, and on the way out the eight coats are returned to the eight people completely at random by an incompetent clerk. What is the probability that no-one gets the correct coat? This is a "classical" example, known as the *derangement problem*.

Of course, we want to solve the derangement problem not just for $n = 8$ people, but for any value of $n$. To state the problem in mathematically precise language, imagine that the people are listed $P_1$, $P_2$, ..., $P_n$ in any arbitrary order. We can record who gets whose coat by a sequence of numbers $(c_1, c_2, ..., c_n)$ in which $c_i = j$ means that $P_i$ was given the coat belonging to $P_j$. The sequence $(c_1, c_2, ..., c_n)$ will thus contain each of the numbers $1, 2, ..., n$ exactly once in some order. In other words, $(c_1, ..., c_n)$ is a permutation of the set $\{1, 2, ..., n\}$, and we assume that this permutation is chosen randomly by the incompetent clerk. Person $i$ gets the correct coat exactly when $c_i = i$. Thus, in general the derangement problem is to determine – for a random permutation $(c_1, ..., c_n)$ of $\{1, 2, ..., n\}$ – the probability that $c_i \neq i$ for all $1 \leq i \leq n$.

For small values of $n$ the derangement problem can be analyzed directly, but complications arise as $n$ gets larger. In fact, this example is perfectly designed to illustrate the Principle of Inclusion/Exclusion. To see how this applies, for each $1 \leq i \leq n$ let $A_i$ be the set of permutations of $\{1, ..., n\}$ such that $c_i = i$. That is, $A_i$ is the set of ways in which the coats are returned and person $i$ gets the correct coat. From that interpretation, the union of sets $A_1 \cup A_2 \cup \cdots \cup A_n$ is the set of ways in which the coats are returned and **at least one person** gets the correct coat. Therefore, the complementary set of permutations gives

those ways of returning the coats so that **no-one** gets the correct coat. The number of these *derangements of n objects* is thus

$$n! - |A_1 \cup A_2 \cup \cdots \cup A_n|.$$

It remains to apply the Principle of Inclusion/Exclusion to determine $|A_1 \cup \cdots \cup A_n|$. To do this we need to determine $|A_S|$ for every nonempty subset $\varnothing \neq S \subseteq \{1,2,...,n\}$. Consider the example $n = 8$ and $S = \{2,3,6\}$. In this case $A_{\{2,3,6\}} = A_2 \cap A_3 \cap A_6$ is the set of those permutations of $\{1,...,8\}$ such that $c_2 = 2$ and $c_3 = 3$ and $c_6 = 6$. Such a permutation looks like $\square$ 2 3 $\square$ $\square$ 6 $\square$ $\square$ where the boxes are filled with the numbers $\{1,4,5,7,8\}$ in some order. Since there are 5! permutations of $\{1,4,5,7,8\}$ it follows that $|A_{\{2,3,6\}}| = 5! = 120$ in this case. The general case is similar. If $\varnothing \neq S \subseteq \{1,2,...,n\}$ is a $k$–element subset then the permutations of $\{1,2,...,n\}$ in $A_S$ are obtained by fixing $c_i = i$ for all $i \in S$, and permuting the remaining $n-k$ elements of $\{1,...,n\} \setminus S$ among themselves. Since there are $(n-k)!$ such permutations we see that $|A_S| = (n-k)!$.

Since $|A_S| = (n-k)!$ for every $k$–element subset of $\{1,2,...,n\}$ – and there are $\binom{n}{k}$ such $k$–element subsets – the Principle of Inclusion/Exclusion implies that

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| &= \sum_{\varnothing \neq S \subseteq \{1,...,n\}} (-1)^{|S|-1} |A_S| \\ &= \sum_{k=1}^{n} \binom{n}{k} (-1)^{k-1} (n-k)! = n! \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}. \end{aligned}$$

Finally, it follows that the number of derangements of $n$ objects is

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

Since the total number of permutations of $n$ objects is $n!$, the probability that a randomly chosen permutation of $\{1,2,...,n\}$ is a derangement is

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

The following table lists the first several values of the function $D_n$ (with the decimals rounded to six places).

| $n$ | $D_n$ | $D_n$ |
|---|---|---|
| 0 | 1/1 | 1. |
| 1 | 0/1 | 0.000000 |
| 2 | 1/2 | 0.500000 |
| 3 | 1/3 | 0.333333 |
| 4 | 3/8 | 0.375000 |
| 5 | 11/30 | 0.366667 |
| 6 | 53/144 | 0.368056 |
| 7 | 103/280 | 0.367857 |
| 8 | 2119/5760 | 0.367882 |
| 9 | 16687/45630 | 0.367879 |
| 10 | 16481/44800 | 0.367879 |

Notice that for $n \geq 7$ the value of $D_n$ changes very little. If you recall the Taylor series expansion of the exponential function

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

then it is easy to see that as $n$ tends to infinity the probability $D_n$ approaches the limiting value of $e^{-1} = 0.3678794412....$

In summary, for the original $n = 8$ derangement problem, the probability that no-one gets their own coat is very close to 36.79%.

## 2.3 Exercises.

**Exercise 2.1** Counting poker hands.
(a) Count straight flushes.
(b) Count quads.
(c) Count full houses.
(d) Count flushes.
(e) Count trips.
(f) Count two pairs.
(g) Count one pairs.

■

**Exercise 2.2** Fix $n \geq 1$ and $1 \leq k \leq t$. Among all multisets of size $n$ with elements of $t$ types, what is the probability that a randomly chosen one has exactly $k$ types that occur with multiplicity at least one? ■

**Exercise 2.3** For $n \geq 1$ and $t \geq 2$, show that:

$$\binom{n+t-1}{t-1} = \sum_{k=0}^{n} \binom{n-k+t-2}{t-2}.$$

■

**Exercise 2.4** ■

**Exercise 2.5** ■

**Exercise 2.6** ■

**Exercise 2.7** ■

**Exercise 2.8** ■

# 3. The Idea of Generating Functions.

We will be dealing algebraically with infinite power series $G(x) = \sum_{n=0}^{\infty} g_n x^n$ in which the coefficients $\mathbf{g} = (g_0, g_1, g_2, \ldots)$ form a sequence of integers. These can, for the most part, be handled just like polynomials. Problems of convergence can arise if one tries to substitute a particular real or complex value for the indeterminate $x$. We usually don't do this, and finiteness of all the coefficients of $G(x)$ is all that we require.

▪ **Example 3.1 — The Geometric Series.** The simplest infinite case of power series is if all the coefficients equal one. Then

$$G = 1 + x + x^2 + x^3 + x^4 + \cdots .$$

Multiply this by $x$:

$$xG = x + x^2 + x^3 + x^4 + \cdots .$$

It follows that $G - xG = (1-x)G = 1$. In conclusion

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

▪

Don't worry about convergence – this is just algebra!

## 3.1 The Binomial Theorem and Binomial Series.

This section develops two of the most useful facts we will need from now on.

**Theorem 3.1.1 — The Binomial Theorem.** For any natural number $n$,

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

This formula is an identity between two polynomials in the variable $x$. You probably have seen a proof of it by induction on $n$, but we are going to prove it here using the bijection between subsets and indicator vectors discussed in Example 2.4.

*Proof.* Recall that $\mathcal{P}(n)$ is the set of all subsets of $\{1,2,...,n\}$, and that $\{0,1\}^n$ is the set of all indicator vectors $\alpha = (a_1, a_2, ..., a_n)$ in which each coordinate is either 0 or 1. Example 2.4 gives a bijection between these two sets, which you should recall. For example, when $n = 8$ the subset $\{2,3,5,7\}$ corresponds to the indicator vector $(0,1,1,0,1,0,1,0)$. The constructions $S \mapsto \alpha(S)$ and $\alpha \mapsto S(\alpha)$ are mutually inverse bijections between the sets $\mathcal{P}(n)$ and $\{0,1\}^n$. From this, we concluded that $|\mathcal{P}(n)| = |\{0,1\}^n| = 2^n$, but we can deduce more. Notice that if $S$ is a subset with $k$ elements then it corresponds to an indicator vector $\alpha$ that sums to $k$. It is sometimes helpful to record this information in a little table, like this:

$$\begin{array}{rcl} \mathcal{P}(n) & \rightleftharpoons & \{0,1\}^n \\ S & \leftrightarrow & \alpha = (a_1, a_2, ..., a_n) \\ |S| & = & a_1 + a_2 + \cdots + a_n. \end{array}$$

Because of this bijection, if we introduce a variable $x$, and if $S$ corresponds to $\alpha$, then

$$x^{|S|} = x^{a_1+a_2+\cdots+a_n}.$$

Moreover, also because of this bijection, summing over all subsets is equivalent to summing over all indicator functions. That is,

$$\sum_{S \in \mathcal{P}(n)} x^{|S|} = \sum_{\alpha \in \{0,1\}^n} x^{a_1+a_2+\cdots+a_n}.$$

Now we can simplify both sides separately. On the LHS, we know from Theorem 2.1.4 that there are $\binom{n}{k}$ $k$-element subsets of an $n$-element set, for each $0 \le k \le n$. Therefore,

$$\sum_{S \in \mathcal{P}(n)} x^{|S|} = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

On the RHS, summing over all the indicator vectors $\alpha \in \{0,1\}^n$ is equivalent to summing over all $a_1 \in \{0,1\}$ and all $a_2 \in \{0,1\}$ and so on,... until all $a_n \in \{0,1\}$. This gives

$$\begin{aligned} \sum_{\alpha \in \{0,1\}^n} x^{a_1+a_2+\cdots+a_n} &= \sum_{a_1=0}^{1} \sum_{a_2=0}^{1} \cdots \sum_{a_n=0}^{1} x^{a_1+a_2+\cdots+a_n} \\ &= \sum_{a_1=0}^{1} x^{a_1} \sum_{a_2=0}^{1} x^{a_2} \cdots \sum_{a_n=0}^{1} x^{a_n} \\ &= \left( \sum_{a=0}^{1} x^a \right)^n = (1+x)^n. \end{aligned}$$

This proves the Binomial Theorem. With practice and familiarity, it becomes a one-line proof:

$$\sum_{k=0}^{\infty}\binom{n}{k}x^k = \sum_{S\in\mathcal{P}(n)} x^{|S|} = \sum_{\alpha\in\{0,1\}^n} x^{a_1+a_2+\cdots+a_n} = (1+x)^n.$$

■

■ **Example 3.2 — Vandermonde Convolution..** As mentioned above, the Binomial Theorem easily implies the Vandermonde Convolution formula. To see this, begin with the obvious identity of polynomials

$$(1+x)^{m+n} = (1+x)^m \cdot (1+x)^n$$

and use the Binomial Theorem to expand each of the factors.

$$\begin{aligned}\sum_{k=0}^{m+n}\binom{m+n}{k}x^k &= \left(\sum_{j=0}^{m}\binom{m}{j}x^j\right)\left(\sum_{i=0}^{n}\binom{n}{i}x^i\right)\\ &= \sum_{j=0}^{m}\sum_{i=0}^{n}\binom{m}{j}\binom{n}{i}x^{j+i}\\ &= \sum_{k=0}^{m+n}\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}x^k.\end{aligned}$$

(The last step is accomplished by re-indexing the double summation.) Since the polynomials on the LHS and on the RHS are equal, they must have the same coefficients. By comparing the coefficients of $x^k$ on both sides we see that

$$\binom{m+n}{k} = \sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j},$$

giving the result. ■

■ **Example 3.3 — The Binomial Series.** Consider the set $\mathcal{M}(t)$ of all multisets with $t$ types of elements, regardless of the size of the multiset. That is, an element of $\mathcal{M}(t)$ is a sequence $\mu = (m_1, m_2, \ldots, m_t)$ of $t$ natural numbers, and the size of the multiset is $|\mu| = n = m_1 + m_2 + \cdots + m_t$. So $\mathcal{M}(t) = \mathbb{N}^t$ is the Cartesian product of $t$ copies of the natural numbers $\mathbb{N}$. We have seen in Theorem 2.1.5 that there are $\binom{n+t-1}{t-1}$ multisets of size $n$ with $t$ types of element. This leads to a calculation similar to the proof of the Binomial Theorem above.

**Theorem 3.1.2** For all integers $t \geq 1$,

$$\frac{1}{(1-x)^t} = \sum_{n=0}^{\infty}\binom{n+t-1}{t-1}x^n.$$

*Proof.* We use the combinatorics of multisets to calculate as follows.

$$\begin{aligned}\sum_{n=0}^{\infty}\binom{n+t-1}{t-1}x^n &= \sum_{\mu\in\mathcal{M}(t)} x^{|\mu|} = \sum_{(m_1,m_2,\ldots,m_t)\in\mathbb{N}^t} x^{m_1+m_2+\cdots m_t}\\ &= \sum_{m_1=0}^{\infty}\sum_{m_2=0}^{\infty}\cdots\sum_{m_t=0}^{\infty} x^{m_1+m_2+\cdots+m_t}\\ &= \sum_{m_1=0}^{\infty} x^{m_1}\sum_{m_2=0}^{\infty} x^{m_2}\cdots\sum_{m_t=0}^{\infty} x^{m_t}\\ &= \left(\sum_{m=0}^{\infty} x^m\right)^t = \frac{1}{(1-x)^t}.\end{aligned}$$

Here we have used the geometric series $1+x+x^2+x^3+\cdots = 1/(1-x)$. ■

This example is the *binomial series* with negative integer exponent. The general binomial series is discussed in Section **??**. ▪

## 3.2 The Theory in General.

In general terms we have a sequence of numbers $\mathbf{g} = (g_0, g_1, g_2, \ldots)$ which we would like to determine. To do this we introduce a variable $x$ and encode these numbers as the coefficients of a power series

$$G(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3 + \cdots = \sum_{n=0}^{\infty} g_n x^n,$$

called the *generating function* for the sequence $\mathbf{g}$. In this section and the next we will see how to use this strategy to encode the answers to various counting problems as generating functions. In the next chapter we will see how to get numbers out of these power series in order to answer the counting problems explicitly.

In this section, the essential definitions are given in subsection 3.2.1. Subsections 3.2.2 to 3.2.4 give technical facts which can be skimmed through at a first pass. They will be used constantly, at which point you can return to them for a deeper understanding.

### 3.2.1 Generating Functions.

Let $\mathcal{A}$ be a set of "objects" which we want to count. For example, $\mathcal{A}$ might be the set of subsets of the set $\{1,2,\ldots,n\}$. Or, $\mathcal{A}$ might be the set of all multisets with $t$ types of elements. The set $\mathcal{A}$ can be quite arbitrary, but we assume that each element of $\mathcal{A}$ has a "size" or "weight" attached to it. The weight of $\alpha \in \mathcal{A}$ is a nonnegative integer $\omega(\alpha) \in \mathbb{N}$. We just require that there are only finitely many elements of $\mathcal{A}$ of any given weight.

**Definition 3.2.1 — Weight Function.** Let $\mathcal{A}$ be a set and let $\omega : \mathcal{A} \to \mathbb{N}$ be a function from $\mathcal{A}$ to the set $\mathbb{N}$ of natural numbers. We say that $\omega$ is a *weight function* provided that for all $n \in \mathbb{N}$, the set

$$\mathcal{A}_n = \omega^{-1}(n) = \{\alpha \in \mathcal{A} : \ \omega(\alpha) = n\}$$

is finite. That is, for every $n \in \mathbb{N}$ there are only finitely many $\alpha \in \mathcal{A}$ of weight $n$.

Under this condition we can define the generating function of $\mathcal{A}$ with respect to $\omega$.

**Definition 3.2.2 — Generating Function.** Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$ as in Definition 3.2.1. The *generating function of $\mathcal{A}$ with respect to $\omega$* is

$$\Phi_{\mathcal{A}}^{\omega}(x) = \sum_{\alpha \in \mathcal{A}} x^{\omega(\alpha)}.$$

**Proposition 3.2.1** Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$, and let

$$\Phi_{\mathcal{A}}^{\omega}(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n.$$

Then, for every $n \in \mathbb{N}$, $a_n = |\mathcal{A}_n|$ is the number of elements in $\mathcal{A}$ that have weight $n$.

*Proof.*

$$\begin{aligned} \Phi_{\mathcal{A}}^{\omega}(x) &= \sum_{\alpha \in \mathcal{A}} x^{\omega(\alpha)} = \sum_{n=0}^{\infty} \sum_{\alpha \in \mathcal{A}:\ \omega(\alpha)=n} x^{\omega(\alpha)} \\ &= \sum_{n=0}^{\infty} \sum_{\alpha \in \mathcal{A}_n} x^n = \sum_{n=0}^{\infty} x^n \sum_{\alpha \in \mathcal{A}_n} 1 = \sum_{n=0}^{\infty} |\mathcal{A}_n| x^n. \end{aligned}$$

Thus, for each $n \in \mathbb{N}$, the coefficient of $x^n$ in $\Phi_{\mathcal{A}}^{\omega}(x)$ is the number of elements in $\mathcal{A}$ that have weight $n$. ■

### 3.2.2 The Sum Lemma.

**Lemma 3.2.2 — The Sum Lemma..** Let $\mathcal{A}$ and $\mathcal{B}$ be disjoint sets, so that $\mathcal{A} \cap \mathcal{B} = \varnothing$. Assume that $\omega : (\mathcal{A} \cup \mathcal{B}) \to \mathbb{N}$ is a weight function on the union of $\mathcal{A}$ and $\mathcal{B}$. We may regard $\omega$ as a weight function on each of $\mathcal{A}$ or $\mathcal{B}$ separately (by restriction). Under these conditions,

$$\Phi_{\mathcal{A}\cup\mathcal{B}}^{\omega}(x) = \Phi_{\mathcal{A}}^{\omega}(x) + \Phi_{\mathcal{B}}^{\omega}(x).$$

*Proof.* From the definition of generating functions,

$$\Phi_{\mathcal{A}\cup\mathcal{B}}^{\omega}(x) = \sum_{\sigma \in \mathcal{A}\cup\mathcal{B}} x^{\omega(\sigma)} = \sum_{\sigma \in \mathcal{A}} x^{\omega(\sigma)} + \sum_{\sigma \in \mathcal{B}} x^{\omega(\sigma)} = \Phi_{\mathcal{A}}^{\omega}(x) + \Phi_{\mathcal{B}}^{\omega}(x).$$

(The condition that $\mathcal{A} \cap \mathcal{B} = \varnothing$ is needed for the second equality.) ■

In fact, the above proof can be generalized slightly to give more.

**Lemma 3.2.3 — The Infinite Sum Lemma..** Let $\mathcal{A}_1$, $\mathcal{A}_2$,... be pairwise disjoint sets (so that $\mathcal{A}_i \cap \mathcal{A}_j = \varnothing$ if $i \neq j$), and let $\mathcal{B} = \bigcup_{i=1}^{\infty} \mathcal{A}_i$. Assume that $\omega : \mathcal{B} \to \mathbb{N}$ is a weight function on the union of the $\mathcal{A}_i$-s. We may regard $\omega$ as a weight function on each of $\mathcal{A}_i$

separately (by restriction). Under these conditions,

$$\Phi^{\omega}_{\mathcal{B}}(x) = \sum_{i=1}^{\infty} \Phi^{\omega}_{\mathcal{A}_i}(x).$$

The proof is left as an exercise.

### 3.2.3 The Product Lemma.

**Lemma 3.2.4 — The Product Lemma..** Let $\mathcal{A}$ and $\mathcal{B}$ be sets with weight functions $\omega : \mathcal{A} \to \mathbb{N}$ and $\nu : \mathcal{B} \to \mathbb{N}$, respectively. Define $\theta : \mathcal{A} \times \mathcal{B} \to \mathbb{N}$ by putting $\theta(\alpha,\beta) = \omega(\alpha) + \nu(\beta)$ for all $(\alpha,\beta) \in \mathcal{A} \times \mathcal{B}$. Then $\theta$ is a weight function on $\mathcal{A} \times \mathcal{B}$ and

$$\Phi^{\theta}_{\mathcal{A}\times\mathcal{B}}(x) = \Phi^{\omega}_{\mathcal{A}}(x) \cdot \Phi^{\nu}_{\mathcal{B}}(x).$$

*Proof.* To see that $\theta$ is a weight function, consider any $n \in \mathbb{N}$. There are $n+1$ choices for an integer $0 \leq k \leq n$. For each such $k$, there are only finitely many pairs $(\alpha,\beta) \in \mathcal{A} \times \mathcal{B}$ with $\omega(\alpha) = k$ and $\omega(\beta) = n-k$. It follows that there are only finitely many elements of $\mathcal{A} \times \mathcal{B}$ of weight $n$. Now,

$$\begin{aligned} \Phi^{\theta}_{\mathcal{A}\times\mathcal{B}}(x) &= \sum_{(\alpha,\beta)\in\mathcal{A}\times\mathcal{B}} x^{\theta(\alpha,\beta)} = \sum_{\alpha\in\mathcal{A}} \sum_{\beta\in\mathcal{B}} x^{\omega(\alpha)+\nu(\beta)} \\ &= \sum_{\alpha\in\mathcal{A}} x^{\omega(\alpha)} \sum_{\beta\in\mathcal{B}} x^{\nu(\beta)} = \Phi^{\omega}_{\mathcal{A}}(x) \cdot \Phi^{\nu}_{\mathcal{B}}(x). \end{aligned}$$

■

The Product Lemma can be extended to the Cartesian product of any finite number of sets, by induction on the number of factors. Proof of this is left as an exercise.

### 3.2.4 The String Lemma.

Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$. For any $k \in \mathbb{N}$, the Cartesian product of $k$ copies of $\mathcal{A}$ is denoted by $\mathcal{A}^k$. The entries of $\mathcal{A}^k$ are $k$-tuples $(\alpha_1, \alpha_2, ..., \alpha_k)$ with each $\alpha_i \in \mathcal{A}$. Notice that $\mathcal{A}^0 = \{\varepsilon\}$ is the one-element set whose only element is the unique empty string $\varepsilon = ()$ of length zero. We can define a weight function $\omega_k$ on $\mathcal{A}^k$ by saying that

$$\omega_k(\alpha_1, ..., \alpha_k) = \omega(\alpha_1) + \cdots + \omega(\alpha_k).$$

It is a good exercise to check that this is a weight function. Note that (when $k = 0$) the weight of the empty string is zero. Repeated application of the Product Lemma shows that

$$\Phi^{\omega_k}_{\mathcal{A}^k}(x) = \left(\Phi^{\omega}_{\mathcal{A}}(x)\right)^k.$$

Now we can take the union of $\mathcal{A}^k$ for all $k \in \mathbb{N}$:

$$\mathcal{A}^* = \bigcup_{k=0}^{\infty} \mathcal{A}^k.$$

Notice that the sets in this union are pairwise disjoint, since each $\mathcal{A}^k$ consists of strings with exactly $k$ coordinates. We define a function $\omega^* : \mathcal{A}^* \to \mathbb{N}$ by saying that $\omega^* = \omega_k$ when restricted to $\mathcal{A}^k$.

**Lemma 3.2.5** Let $\mathcal{A}$ be a set with weight function $\omega : \mathcal{A} \to \mathbb{N}$, and define $\mathcal{A}^*$ and $\omega^* : \mathcal{A}^* \to \mathbb{N}$ as above. Then $\omega^*$ is a weight function on $\mathcal{A}^*$ if and only if there are no elements of weight zero in $\mathcal{A}$.

*Proof.* If $\gamma \in \mathcal{A}$ has weight zero, $\omega(\gamma) = 0$, then for any natural number $k \in \mathbb{N}$, a sequence of $k$ $\gamma$-s in $\mathcal{A}^k$ also has weight zero: $\omega_k(\gamma, \gamma, ..., \gamma) = 0$. So, by the way $\omega^* : \mathcal{A}^* \to \mathbb{N}$ is defined, there are infinitely many elements of weight zero in $\mathcal{A}^*$, so that $\omega^*$ is not a weight function.

Conversely, assume that every element of $\mathcal{A}$ has weight at least 1. Then, for each $k \in \mathbb{N}$, every element of $\mathcal{A}^k$ has weight at least $k$. Now consider any $n \in \mathbb{N}$ and all the strings $(\alpha_1, ..., \alpha_k) \in \mathcal{A}^*$ of weight $n$. By the previous sentence, if there are any such strings of length $k$ then $0 \leq k \leq n$. For each $0 \leq k \leq n$, $\mathcal{A}^k$ has only finitely many elements of weight $n$. It follows that $\mathcal{A}^*$ has only finitely many elements of weight $n$. Therefore, $\omega^*$ is a weight function on $\mathcal{A}^*$. ■

**Lemma 3.2.6 — The String Lemma..** Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$ such that there are no elements of $\mathcal{A}$ of weight zero. Then

$$\Phi_{\mathcal{A}^*}^{\omega^*}(x) = \frac{1}{1 - \Phi_{\mathcal{A}}^{\omega}(x)}.$$

*Proof.* By the Infinite Sum and Product Lemmas,

$$\Phi_{\mathcal{A}^*}^{\omega^*}(x) = \sum_{k=0}^{\infty} \Phi_{\mathcal{A}^k}^{\omega_k}(x) = \sum_{k=0}^{\infty} \left(\Phi_{\mathcal{A}}^{\omega}(x)\right)^k = \frac{1}{1 - \Phi_{\mathcal{A}}^{\omega}(x)}.$$

■

## 3.3 Compositions.

**Definition 3.3.1** A *composition* is a finite sequence of positive integers:

$$\gamma = (c_1, c_2, ..., c_k),$$

in which $k \in \mathbb{N}$ is a natural number, and each $c_i \in \mathbb{P}$ is a positive integer. The entries $c_i$ are called the *parts* of the composition. The *length* of the composition is $\ell(\gamma) = k$, the number of parts. The *size* of the composition is

$$|\gamma| = c_1 + c_2 + \cdots + c_k,$$

the sum of the parts.

Notice that there is exactly one composition of length zero: this is $\varepsilon = ()$, the empty string with no entries. Compositions are related to multisets, but there are two important differences: the parts of a composition must be positive integers, not just nonnegative, and the length of a composition can be variable while the number of types of element in a multiset is fixed.

In this section we will apply the theory of generating functions to obtain formulas for the generating functions of various sets of compositions defined by imposing some extra conditions. In the next chapter we will see how to use this information to actually count such things.

**Theorem 3.3.1** 1. The set $\mathcal{C}$ of all compositions is $\mathcal{C} = \mathbb{P}^*$.

2. The generating function for $\mathcal{C}$ with respect to size is

$$C(x) = \Phi_{\mathcal{C}}^{|\cdot|}(x) = 1 + \frac{x}{1-2x}.$$

3. For each $n \in \mathbb{N}$, he number of compositions of size $n$ is

$$|\mathcal{C}_n| = \begin{cases} 1 & \text{if } n = 0, \\ 2^{n-1} & \text{if } n \geq 1. \end{cases}$$

*Proof.* A single part is a positive integer $c \in \mathbb{P} = \{1, 2, 3, ...\}$. A composition of length $k$ is a sequence $\gamma = (c_1, c_2, ..., c_k)$ of $k$ positive integers, so is an element of $\mathbb{P}^k$. Since the length $k$ can be any natural number, the set $\mathcal{C}$ of all compositions is

$$\mathcal{C} = \bigcup_{k=0}^{\infty} \mathbb{P}^k = \mathbb{P}^*.$$

This proves 1.

The generating function for one-part compositions with respect to size is

$$\Phi_{\mathbb{P}}(x) = \sum_{c=1}^{\infty} = x + x^2 + x^3 + \cdots = \frac{x}{1-x},$$

by the geometric series. From the String Lemma 3.2.6 it follows that

$$C(x) = \Phi_{\mathcal{C}}^{|\cdot|}(x) = \frac{1}{1 - (\frac{x}{1-x})} = \frac{1-x}{1-2x} = 1 + \frac{x}{1-2x}.$$

This proves 2.

Expanding $C(x)$ using the geometric series we obtain

$$C(x) = 1 + \sum_{j=0}^{\infty} 2^j x^{j+1} = 1 + \sum_{n=1}^{\infty} 2^{n-1} x^n.$$

Since $|\mathcal{C}_n| = [x^n]C(x)$ is the coefficient of $x^n$ in $C(x)$, this proves 3. ■

Many variations on the proof of Theorem 3.3.1 are possible. We will do a few as examples, and present many more as exercises. The general approach consists of three steps:

- Identify the allowed values for each part. Sometimes this might depend on the position of the part within the composition.
- Identify the allowed lengths for the compositions.

- Apply the Sum, Product, and String Lemmas to obtain a formula for the generating function.

■ **Example 3.4** Let $\mathcal{F}$ be the set of all compositions in which each part is either one or two.

- The allowed sizes for a part are 1 or 2, so $P = \{1,2\}$ is the set of allowed parts. The generating function for a single part is $x+x^2$.
- The length can be any natural number $k \in \mathbb{N}$. By the Product Lemma, the generating function for a composition in $\mathcal{F}$ of length $k$ is $(x+x^2)^k$.
- Since $\mathcal{F} = \{1,2\}^*$, the String Lemma implies that

$$F(x) = \sum_{n=0}^{\infty} f_n x^n = \sum_{k=0}^{\infty} (x+x^2)^k = \frac{1}{1-x-x^2}.$$

Here $|\mathcal{F}_n| = f_n = [x^n]F(x)$ is the number of compositions in $\mathcal{F}$ of size $n$. In Section 4.1 we will see how to use this information to determine the numbers $f_n$.

■

■ **Example 3.5** Let $\mathcal{H}$ be the set of all compositions in which each part is at least two.

- The allowed sizes for a part are $P = \{2,3,4,...\}$. The generating function for a single part is

$$\Phi_P(x) = \sum_{c=2}^{\infty} x^c = x^2 + x^3 + x^4 + \cdots = \frac{x^2}{1-x}.$$

- The length can be any natural number $k \in \mathbb{N}$. By the Product Lemma, the generating function for a composition in $\mathcal{H}$ of length $k$ is

$$\left(\frac{x^2}{1-x}\right)^k.$$

- Since $\mathcal{H} = P^*$, the String Lemma implies that

$$H(x) = \sum_{n=0}^{\infty} h_n x^n = \frac{1}{1-(\frac{x^2}{1-x})} = \frac{1-x}{1-x-x^2} = 1 + \frac{x^2}{1-x-x^2}.$$

Here $|\mathcal{H}_n| = h_n = [x^n]H(x)$ is the number of compositions in $\mathcal{H}$ of size $n$.

■

■ **Example 3.6** Let $\mathcal{J}$ be the set of all compositions in which each part is odd.

- The allowed sizes for a part are $P = \{1,3,5,...\}$. The generating function for a single part is

$$\Phi_P(x) = \sum_{i=0}^{\infty} x^{2i+1} = x^1 + x^3 + x^5 + \cdots = \frac{x}{1-x^2}.$$

- The length can be any natural number $k \in \mathbb{N}$. By the Product Lemma, the generating function for a composition in $\mathcal{J}$ of length $k$ is

$$\left(\frac{x}{1-x^2}\right)^k.$$

- Since $\mathcal{J} = P^*$, the String Lemma implies that

$$J(x) = \sum_{n=0}^{\infty} j_n x^n = \frac{1}{1-(\frac{x}{1-x^2})} = \frac{1-x^2}{1-x-x^2} = 1 + \frac{x}{1-x-x^2}.$$

  Here $|\mathcal{J}_n| = j_n = [x^n]J(x)$ is the number of compositions in $\mathcal{J}$ of size $n$.

■

These three examples have very similar generating functions. In fact, after a little reflection one sees that for all $n \geq 2$

$$[x^n]H(x) = [x^{n-1}]J(x) = [x^{n-2}]F(x) = [x^{n-2}]\frac{1}{1-x-x^2}.$$

This means that for all $n \geq 2$, $h_n = j_{n-1} = f_{n-2}$. So, for the sizes of sets, $|\mathcal{H}_n| = |\mathcal{J}_{n-1}| = |\mathcal{F}_{n-2}|$. We have proven these equalities even though we don't yet know what those numbers actually are! Since these sets have the same sizes there must be bijections between them to explain this fact. Constructing such bijections is left as a good exercise. As a starting point, here are the sets for $n = 7$:

| $\mathcal{H}_7$ | $\mathcal{J}_6$ | $\mathcal{F}_5$ |
|---|---|---|
| $(7)$ | $(5,1)$ | $(2,2,1)$ |
| $(5,2)$ | $(1,5)$ | $(2,1,2)$ |
| $(2,5)$ | $(3,3)$ | $(1,2,2)$ |
| $(4,3)$ | $(3,1,1,1)$ | $(2,1,1,1)$ |
| $(3,4)$ | $(1,3,1,1)$ | $(1,2,1,1)$ |
| $(3,2,2)$ | $(1,1,3,1)$ | $(1,1,2,1)$ |
| $(2,3,2)$ | $(1,1,1,3)$ | $(1,1,1,2)$ |
| $(2,2,3)$ | $(1,1,1,1,1,1)$ | $(1,1,1,1,1)$ |

(It need not be the case that the bijections match up these sets of compositions line by line.)

■ **Example 3.7** Let $\mathcal{Q}$ be the set of all compositions in which each part is at least two, and the number of parts is even.

- The allowed sizes for a part are $P = \{2,3,4,...\}$. The generating function for a single part is

$$\Phi_P(x) = \sum_{c=2}^{\infty} x^c = x^2 + x^3 + x^4 + \cdots = \frac{x^2}{1-x}.$$

- The length is an even natural number $k = 2j$ for some $j \in \mathbb{N}$. By the Product Lemma, the generating function for a composition in $\mathcal{Q}$ of length $2j$ is

$$\left(\frac{x^2}{1-x}\right)^{2j}.$$

- Since $\mathcal{Q} = (P^2)^*$, the String Lemma implies that

$$Q(x) = \sum_{n=0}^{\infty} q_n x^n = \sum_{j=0}^{\infty} \left(\frac{x^2}{1-x}\right)^{2j} = \frac{1}{1-\left(\frac{x^2}{1-x}\right)^2} = \frac{(1-x)^2}{(1-x)^2 - x^4} = \frac{1-2x+x^2}{1-2x+x^2-x^4}.$$

  Here $|\mathcal{Q}_n| = q_n = [x^n]Q(x)$ is the number of compositions in $\mathcal{Q}$ of size $n$. In Theorem 4.2.1 we will see how to calculate the first several values of $|\mathcal{Q}_n|$.

■

## 3.4 Proof of Inclusion/Exclusion.

In this section we prove Theorem 2.1.7, the Principle of Inclusion/Exclusion.

**Lemma 3.4.1** For any nonempty set $T$,

$$\sum_{\varnothing \neq S \subseteq T} (-1)^{|S|-1} = 1.$$

*Proof.* Consider the identity

$$\sum_{S \subseteq \{1,2,\ldots,n\}} x^{|S|} = (1+x)^n$$

which was part of the proof of the Binomial Theorem. If $|T| = n$ then

$$\sum_{S \subseteq T} x^{|S|} = (1+x)^n$$

as well (as can be seen by numbering the elements of $T$ by $t_1, \ldots, t_n$ arbitrarily). Both sides are polynomials, so we can substitute $x = -1$. The result is

$$\sum_{S \subseteq T} (-1)^{|S|} = (1-1)^n = 0$$

since $n \geq 1$. (Note that $0^0 = 1$ since it is an empty product.) On the LHS we separate the term corresponding to $S = \varnothing$, and we see that

$$1 + \sum_{\varnothing \neq S \subseteq T} (-1)^{|S|} = 0.$$

Rearranging this, we see that

$$\sum_{\varnothing \neq S \subseteq T} (-1)^{|S|-1} = 1,$$

completing the proof. ■

Recall the notation from subsection 2.1.9: for any finite number of sets $A_1, A_2, \ldots, A_m$ and $\varnothing \neq S \subseteq \{1, 2, \ldots, m\}$, let

$$A_S = \bigcap_{i \in S} A_i.$$

So, for example, $A_{\{2,3,5\}} = A_2 \cap A_3 \cap A_5$.

**Theorem 3.4.2 — Inclusion/Exclusion.** Let $A_1, A_2, \ldots, A_m$ be finite sets. Then

$$|A_1 \cup \cdots \cup A_m| = \sum_{\varnothing \neq S \subseteq \{1,2,\ldots,m\}} (-1)^{|S|-1} |A_S|.$$

*Proof.* Let $V = A_1 \cup \cdots \cup A_m$, and let $N_m = \{1,2,..,m\}$. For each $v \in V$ let $T(v) := \{i \in N_m : \ v \in A_i\}$. Notice that $T(v) \neq \varnothing$, for all $v \in V$. Also notice that for $\varnothing \neq S \subseteq N_m$ we have $v \in A_S$ if and only if $\varnothing \neq S \subseteq T(v)$. Therefore, using Lemma 3.4.1 above,

$$\begin{aligned}\sum_{\varnothing \neq S \subseteq N_m} (-1)^{|S|-1}|A_S| &= \sum_{\varnothing \neq S \subseteq N_m} (-1)^{|S|-1} \sum_{v \in A_S} 1 \\ &= \sum_{v \in V} \sum_{\varnothing \neq S \subseteq T(v)} (-1)^{|S|-1} = \sum_{v \in V} 1 = |V|,\end{aligned}$$

as was to be shown. ■

■ **Example 3.8** For a positive integer $n$, the *Euler totient* of $n$ is the number $\varphi(n)$ of integers $b$ in the range $1 \leq b \leq n$ such that $b$ and $n$ are relatively prime. That is,

$$\varphi(n) = |\{b \in \{1,2,...,n\} : \ \gcd(b,n) = 1\}|.$$

We can use Inclusion/Exclusion to obtain a formula for $\varphi(n)$, as follows. Let the prime factorization of $n$ be $n = p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$, in which the $p_i$ are pairwise distinct primes and the $c_i$ are positive integers. For each $1 \leq i \leq m$, let

$$A_i := \{b \in N_n : \ p_i \text{ divides } b\}.$$

Then

$$\varphi(n) = |(N_n \setminus (A_1 \cup \cdots \cup A_m))| = n - |A_1 \cup \cdots \cup A_m|.$$

Since the factors $p_i$ are pairwise coprime, for any $\varnothing \neq S \subseteq N_m$ and $b \in N_n$ we have $b \in A_S$ if and only if $\prod_{i \in S} p_i$ divides $b$. Therefore,

$$|A_S| = \frac{n}{\prod_{i \in S} p_i}.$$

By Inclusion/Exclusion, it follows that

$$|A_1 \cup \cdots \cup A_m| = n \sum_{\varnothing \neq S \subseteq N_m} (-1)^{|S|-1} \prod_{i \in S} \frac{1}{p_i}.$$

Therefore

$$\begin{aligned}\varphi(n) &= n - n \sum_{\varnothing \neq S \subseteq N_m} (-1)^{|S|-1} \prod_{i \in S} \frac{1}{p_i} \\ &= n \sum_{S \subseteq N_m} (-1)^{|S|} \prod_{i \in S} \frac{1}{p_i} = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).\end{aligned}$$

■

## 3.5 Exercises.

**Exercise 3.1** Let $\mathcal{W}$ be the set of compositions $\gamma = (c_1, c_2, ..., c_k)$ in which the length is

arbitrary, and such that $c_i$ is even when $i$ is even, and $c_i$ is odd when $i$ is odd. Show that

$$W(x) = \Phi_W^{|\cdot|}(x) = 1 + \frac{x}{1 - 2x^2 - x^3 + x^4}.$$

■

# 4. Linear Recurrence Relations.

In Chapter 3 we saw how to encode a sequence of numbers as the coefficients of a power series $G(x) = \sum_{n=0}^{\infty} g_n x^n$. We used the Sum, Product, and String Lemmas to obtain algebraic formulas for these generating functions. In this section we will see one technique for using these algebraic formulas to compute the coefficients $g_n$, which are the numbers we really want. First we will do the example of Fibonacci numbers in detail, and then we will develop the general theory.

## 4.1 Fibonacci Numbers.

**Definition 4.1.1** The sequence of *Fibonacci numbers* $\mathbf{f} = (f_0, f_1, f_2, f_3, \ldots)$ is defined by putting $f_0 = 1$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. One can use this information to compute $f_n$ iteratively for as long as you want:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_n$ | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 |

Although this definition determines the sequence precisely, it does not give an exact formula for the number $f_n$ as a function of $n$. We obtain such a formula in this section. Moreover, this is just the first example of a very general technique, which is the subject of this chapter.

To begin with, we obtain a formula for the generating function $F(x) = \sum_{n=0}^{\infty} f_n x^n$.

■ **Example 4.1** To use the information defining the Fibonacci numbers, we begin by writing

$$F(x) = f_0 + f_1 x + \sum_{n=2}^{\infty} f_n x^n = 1 + x + \sum_{n=2}^{\infty} (f_{n-1} + f_{n-2}) x^n.$$

The next step is to write the RHS in terms of $F(x)$. This is done by re-indexing the

summation(s).

$$\begin{aligned} F(x) &= 1+x+\sum_{n=2}^{\infty}(f_{n-1}+f_{n-2})x^n \\ &= 1+x+\sum_{n=2}^{\infty}f_{n-1}x^n+\sum_{n=2}^{\infty}f_{n-2}x^n \\ &= 1+x+x\sum_{i=1}^{\infty}f_i x^i+x^2\sum_{j=0}^{\infty}f_j x^j \\ &= 1+x+x(F(x)-f_0)+x^2F(x) \\ &= 1+xF(x)+x^2F(x). \end{aligned}$$

This equation can be solved for $F(x)$, yielding

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

■

We have seen this generating function before, relating to the sets of compositions $\mathcal{F}$, $\mathcal{H}$, and $\mathcal{J}$ at the end of Section 3.3. Obtaining a formula for Fibonacci numbers will thus solve the counting problem for each of these sets of compositions.

As in the general case, the key is the denominator of the generating function – in this case $1-x-x^2$. We start by factoring it in the form

$$1-x-x^2=(1-\alpha x)(1-\beta x)$$

for some complex numbers $\alpha$ and $\beta$, the *inverse roots* of the polynomial. To do this we can use the Quadratic Formula, but since we are looking for the inverse roots of a quadratic polynomial we have to be careful. Substitute $x=1/z$ and multiply both sides by $z^2$ to get

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

Now the roots of this polynomial are given by the Quadratic Formula:

$$\left.\begin{matrix}\alpha\\ \beta\end{matrix}\right\}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}=\frac{1\pm\sqrt{5}}{2}.$$

The next step is to apply the Theorem of Partial Fractions, which will be explained in Section 4.3. In this case it states that there are complex numbers $A$ and $B$ such that

$$F(x)=\sum_{n=0}^{\infty}f_nx^n=\frac{1}{1-x-x^2}=\frac{1}{(1-\alpha x)(1-\beta x)}=\frac{A}{1-\alpha x}+\frac{B}{1-\beta x}.$$

There are a few different ways to find the coefficients $A$ and $B$, as we will see later in this chapter. Here we can multiply by $1-x-x^2=(1-\alpha x)(1-\beta x)$ and collect like powers of $x$:

$$1=A(1-\beta x)+B(1-\alpha x)=(A+B)-(A\beta+B\alpha)x.$$

We see that $A+B=1$ and $A\beta+B\alpha=0$. Subtracting the second of these equations from $A\alpha+B\alpha=\alpha$ we see that

$$A=\frac{\alpha}{\alpha-\beta}=\frac{5+\sqrt{5}}{10}.$$

Similarly, from $A\beta + B\beta = \beta$ and $A\beta + B\alpha = 0$ we see that

$$B = \frac{\beta}{\beta - \alpha} = \frac{5-\sqrt{5}}{10}.$$

Now we can expand the geometric series above, with the result that

$$\begin{aligned} F(x) &= \sum_{n=0}^{\infty} f_n x^n = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x} \\ &= A\sum_{n=0}^{\infty} \alpha^n x^n + B\sum_{n=0}^{\infty} \beta^n x^n = \sum_{n=0}^{\infty} (A\alpha^n + B\beta^n) x^n. \end{aligned}$$

It follows that for all $n \in \mathbb{N}$, the Fibonacci numbers are given by the formula

$$f_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

That seems kind of weird, since we know that the Fibonacci numbers are integers. But notice that $\beta = (1-\sqrt{5})/2 \approx -0.618$ so that as $n \to \infty$, $\beta^n \to 0$. In fact $f_n$ is the integer closest to $\frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n$ for all $n \in \mathbb{N}$.

## 4.2 Homogeneous Linear Recurrence Relations.

**Definition 4.2.1** Let $\mathbf{g} = (g_0, g_1, g_2, \ldots)$ be an infinite sequence of integers. The corresponding generating function is $G(x) = g_0 + g_1 x + g_2 x^2 + \cdots = \sum_{n=0}^{\infty} g_n x^n$. Let $a_1$, $a_2$,... $a_d$ be integers, and let $N \geq d$ be a natural number. We say that $\mathbf{g}$ satisfies a *homogeneous linear recurrence relation* provided that

$$g_n + a_1 g_{n-1} + a_2 g_{n-2} + \cdots + a_d g_{n-d} = 0$$

for all $n \geq N$. The values $g_0, g_1, \ldots g_{N-1}$ are the *initial conditions* of the recurrence.

The relation is *linear* because it is a linear combination of the entries of the sequence $\mathbf{g}$; it is *homogeneous* because the RHS of the equation is zero.

The recurrence relation can be rewritten as

$$g_n = -(a_1 g_{n-1} + a_2 g_{n-2} + \cdots + a_d g_{n-d})$$

for all $n \geq N$, and this can be used to compute the numbers $g_n$ by induction on $n$. In Chapter 7 we will have a brief look at recurrence relations which are not linear.

Consider the example of Fibonacci numbers above: $f_0 = f_1 = 1$ are the initial conditions, and $f_n - f_{n-1} - f_{n-2} = 0$ for all $n \geq 2$ is a homogeneous linear recurrence relation. We have the formula

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

for the generating function. This is an instance of a general fact about sequences with homogeneous linear recurrence relations. Let's do another example before going to the general theory.

■ **Example 4.2** *Define a sequence* $\mathbf{g} = (g_0, g_1, \ldots)$ *by the initial conditions* $g_0 = 2$, $g_1 = 5$, *and* $g_2 = 6$, *and the recurrence relation* $g_n - 3g_{n-2} - 2g_{n-3} = 0$ *for all* $n \geq 3$. *Obtain a formula for the generating function* $G(x) = \sum_{n=0}^{\infty} g_n x^n$.
The general method is to multiply the recurrence by $x^n$ and sum over all $n \geq N$. In this case

$$\sum_{n=3}^{\infty} (g_n - 3g_{n-2} - 2g_{n-3})\, x^n = 0.$$

Now we split the LHS into separate summations, reindex them, and write everything in terms of the power series $G(x)$

$$\begin{aligned}
\sum_{n=3}^{\infty} g_n x^n - 3\sum_{n=3}^{\infty} g_{n-2}x^n - 2\sum_{n=3}^{\infty} g_{n-3}x^n &= 0 \\
(G(x) - g_0 - g_1 x - g_2 x^2) - 3x^2 \sum_{j=1}^{\infty} g_j x^j - 2x^3 \sum_{k=0}^{\infty} g_k x^k &= 0 \\
(G(x) - 2 - 5x - 6x^2) - 3x^2(G(x) - 2) - 2x^3 G(x) &= 0 \\
G(x) - 3x^2 G(x) - 2x^3 G(x) &= 2 + 5x.
\end{aligned}$$

It follows that

$$G(x) = \frac{2 + 5x}{1 - 3x^2 - 2x^3}.$$

Notice how the polynomial $1 - 3x^2 - 2x^3$ in the denominator of this formula is related to the linear recurrence relation $g_n - 3g_{n-2} - 2g_{n-3} = 0$ for $n \geq 3$. We can explain the numerator, too, if we make the convention that $g_n = 0$ for all integers $n < 0$. Then, using the initial conditions, we have

$$\begin{aligned}
g_0 - 3g_{-2} - 2g_{-3} &= 2 - 0 - 0 = 2 \text{ for } n = 0, \\
g_1 - 3g_{-1} - 2g_{-2} &= 5 - 0 - 0 = 5 \text{ for } n = 1, \\
g_2 - 3g_0 - 2g_{-1} &= 6 - 3 \cdot 2 - 0 = 0 \text{ for } n = 2, \\
g_n - 3g_{n-2} - 2g_{n-3} &= 0 \text{ for } n \geq 3.
\end{aligned}$$

■

**Theorem 4.2.1** Let $\mathbf{g} = (g_0, g_1, g_2)$ be a sequence of integers, and let $G(x) = \sum_{n=0}^{\infty} g_n x^n$ be the corresponding generating function. The following are equivalent:

1. $\mathbf{g}$ satisfies a homogeneous linear recurrence relation

   $$g_n + a_1 g_{n-1} + \cdots + a_d g_{n-d} = 0 \text{ for all } n \geq N,$$

   with initial conditions $g_0$, $g_1$,..., $g_{N-1}$.
2. $G(x) = P(x)/Q(x)$ is a quotient of two polynomials. The denominator is

   $$Q(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

   and the numerator is $P(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{N-1} x^{N-1}$ where

   $$b_k = g_k + a_1 g_{k-1} + \cdots + a_d g_{k-d}$$

for all $0 \leq k \leq N-1$, with the convention that $g_n = 0$ for all $n < 0$.

*Proof.* To prove this theorem, we just copy the calculation in Example 4.2 but do it in the most general case. For convenience, let $a_0 = 1$. Assume that part 1. holds, and let

$$Q(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_d x^d.$$

Consider the product $Q(x)G(x)$:

$$\begin{aligned} Q(x)G(x) &= \left(\sum_{j=0}^{d} a_j x^j\right)\left(\sum_{n=0}^{\infty} g_n x^n\right) \\ &= \sum_{j=0}^{d}\sum_{n=0}^{\infty} a_j g_n x^{n+j} = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{d} a_j g_{k-j}\right) x^k. \end{aligned}$$

In the last step we have re-indexed the double sum using $k = n + j$, and used the convention that $g_n = 0$ for all $n < 0$.

The coefficient of $x^k$ in this formula is the recurrence relation for $\mathbf{g}$ applied when $n = k$. Thus, this coefficient is zero for $k \geq N$. On the other hand, for $0 \leq k \leq N-1$, we see that $\sum_{j=0}^{d} a_j g_{k-j} = b_k$ by the way the numbers $b_k$ were definined in part 2. That is,

$$Q(x)G(x) = \sum_{k=0}^{N-1} b_k x^k = P(x),$$

and it follows that $G(x) = P(x)/Q(x)$. This shows that 1. implies 2.

Conversely, assume that 2. holds and that $G(x) = P(x)/Q(x)$ is as given. We can use $b_k = g_k + a_1 g_{k-1} + \cdots + a_d g_{k-d}$ for $0 \leq k \leq N-1$ to determine the initial conditions $g_0$, $g_1$,... $g_{N-1}$ inductively. Then the facts that $Q(x)G(x) = P(x)$ and that the degree of $P(x)$ is at most $N-1$ implies that

$$g_k + a_1 g_{k-1} + \cdots + a_d g_{k-d} = 0 \text{ for all } k \geq N.$$

This shows that 2. implies 1. ■

Theorem 4.2.1 is useful in both directions, as the following two examples show.

■ **Example 4.3** *Let*

$$D(x) = \sum_{n=0}^{\infty} d_n x^n = \frac{1 - 3x + 4x^2}{1 - 2x + 3x^3}.$$

*Obtain a homogeneous linear recurrence relation satisfied by* $\mathbf{d} = (d_0, d_1, d_2, \ldots)$.

From Theorem 4.2.1 we can read off immediately that for all $n \in \mathbb{N}$:

$$d_n - 2d_{n-1} + 3d_{n-3} = \begin{cases} 1 & \text{if } n = 0, \\ -3 & \text{if } n = 1, \\ 4 & \text{if } n = 2, \\ 0 & \text{if } n \geq 3, \end{cases}$$

with the convention that $d_n = 0$ if $n < 0$. We can determine the initial conditions inductively as follows: $d_0 = 1$; $d_1 - 2d_0 = -3$, so $d_1 = -1$; $d_2 - 2d_1 = 4$, so $d_2 = 2$. The recurrence

$d_n - 2d_{n-1} + 3d_{n-3} = 0$ holds for all $n \geq 3$. Using the initial coditions $d_0 = 1$, $d_1 = -1$, $d_2 = 2$, and the recurrence $d_n = 2d_{n-1} - 3d_{n-3}$ for all $n \geq 3$, we can compute $d_n$ for as long as we want:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $d_n$ | 1 | −1 | 1 | 1 | 5 | 4 | 5 | −5 | −22 |

■

■ **Example 4.4** *A sequence* $\mathbf{s} = (s_0, s_1, s_2, ...)$ *is defined by the initial conditions* $s_0 = 1$, $s_1 = 2$, $s_2 = 1$, *and the recurrence* $s_n - s_{n-1} - 2s_{n-3} = 0$ *for all* $n \geq 3$. *Obtain a formula for the generating function* $S(x) = \sum_{n=0}^{\infty} s_n x^n$.

Since we have the information at hand, we might as well compute a few more values of $s_n$:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $s_n$ | 1 | 2 | 1 | 3 | 7 | 9 | 15 | 29 |

To get the generating function, Theorem 4.2.1 implies immediately that the denominator is $1 - x - 2x^3$. To obtain the numerator we apply the recurrence for small values of $n$, with the convention that $s_n = 0$ if $n < 0$.

$$s_n - s_{n-1} - 2s_{n-3} = \begin{cases} 1 & \text{if } n = 0, \\ 2 - 1 & \text{if } n = 1, \\ 1 - 2 & \text{if } n = 2. \end{cases}$$

Thus, the numerator is $1 + x - x^2$. The generating function is

$$S(x) = \frac{1 + x - x^2}{1 - x - 2x^3}.$$

■

■ **Example 4.5** Let's revisit Example **??**, concerning the set $\mathcal{Q}$ of all compositions in which each part is at least two, and the number of parts is even. We derived the generating function

$$Q(x) = \sum_{n=0}^{\infty} q_n x^n = \frac{1 - 2x + x^2}{1 - 2x + x^2 - x^4}.$$

From Theorem 4.2.1 we see immediately that

$$q_n - 2q_{n-1} + q_{n-2} - q_{n-4} = \begin{cases} 1 & \text{if } n = 0, \\ -2 & \text{if } n = 1, \\ 1 & \text{if } n = 2, \\ 0 & \text{if } n \geq 3, \end{cases}$$

with the convention that $q_n = 0$ if $n < 0$. We can inductively calculate the first several values of $q_n$:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $q_n$ | 1 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 6 | 10 | 17 | 28 | 45 | 72 | 116 |

We have determined that $|\mathcal{Q}_{14}| = 116$, but we have not listed all these compositions individually. ■

## 4.3 Partial Fractions.

**Theorem 4.3.1 — Partial Fractions.** Let $F(x) = P(x)/Q(x)$ be a quotient of polynomials in which $\deg P < \deg Q$ and the constant term of $Q(x)$ is 1. Factor the denominator to obtain its inverse roots:

$$Q(x) = (1-\lambda_1 x)^{d_1}(1-\lambda_2 x)^{d_2}\cdots(1-\lambda_s x)^{d_s}$$

in which $\lambda_1, ..., \lambda_s$ are distinct nonzero complex numbers and $d_1 + \cdots + d_s = d = \deg Q$. Then there are $d$ complex numbers:

$$C_1^{(1)}, C_1^{(2)}, ..., C_1^{(d_1)};\ C_2^{(1)}, C_2^{(2)}, ..., C_2^{(d_2)};\ \ldots;\ C_s^{(1)}, C_s^{(2)}, ..., C_s^{(d_s)};$$

(which are uniquely determined) such that

$$F(x) = \frac{P(x)}{Q(x)} = \sum_{i=1}^{s}\sum_{j=1}^{d_s}\frac{C_i^{(j)}}{(1-\lambda_i x)^j}.$$

*Proof.* Consider the set $\mathcal{V}_Q$ of all quotients of polynomials $P(x)/Q(x)$ in which $\deg P < d = \deg Q$, where the denominator is some polynomial which remains fixed throughout the proof and satisfies the hypothesis of the theorem. It is easily seen that $\mathcal{V}_Q$ is a vector space over the complex numbers $\mathbb{C}$, since if $P(x)$ and $R(x)$ both have degree less than $d$ and $\alpha \in \mathbb{C}$ then $P(x) + \alpha R(x)$ has degree less than $d$. It is also clear that the vectors

$$\frac{1}{Q(x)},\ \frac{x}{Q(x)},\ \frac{x^2}{Q(x)},\ \ldots,\ \frac{x^{d-1}}{Q(x)}$$

span $\mathcal{V}_Q$ as a vector space over $\mathbb{C}$. Therefore, the dimension of $\mathcal{V}_Q$ is at most $d$.

Now we claim that for every $1 \le i \le s$ and $1 \le j \le d_i$, the quotient $1/(1-\lambda_i x)^j$ is in $\mathcal{V}_Q$. This is because

$$\frac{1}{(1-\lambda_i x)^j} = \frac{(1-\lambda_i x)^{d_i - j}\prod_{h\neq i}(1-\lambda_h x)^{d_h}}{Q(x)}$$

and the numerator has degree $d - j \le d - 1 < d$.

The essential point in the proof is that the set of vectors

$$\mathcal{B} = \left\{\frac{1}{(1-\lambda_i x)^j} :\ 1 \le i \le s \text{ and } 1 \le j \le d_i\right\}$$

in $\mathcal{V}_Q$ is linearly independent. From this we can conclude that the dimension of $\mathcal{V}_Q$ is at least $d_1 + \cdots + d_s = d$. It then follows that $\dim \mathcal{V}_Q = d$ and that $\mathcal{B}$ is a basis for $\mathcal{V}_Q$. Therefore, every vector in $\mathcal{V}_Q$ can be written uniquely as a linear combination of vectors in $\mathcal{B}$. That is exactly what the Partial Fractions Theorem is claiming.

It remains only to show that $\mathcal{B}$ is a linearly independent set. Consider any linear combination of vectors in $\mathcal{B}$ which gives the zero vector:

$$\sum_{i=1}^{s}\sum_{j=1}^{d_s}\frac{C_i^{(j)}}{(1-\lambda_i x)^j} = 0. \tag{4.1}$$

We must show that $C_i^{(j)} = 0$ for all $1 \le i \le s$ and $1 \le j \le d_i$. Suppose not. Then there is some coefficient $C_p^{(t)} \neq 0$ with $1 \le p \le s$ and $1 \le t \le d_p$ which also satisfies $C_p^{(t+1)} = \cdots = C_p^{(d_p)} = 0$. Now multiply equation 4.1 by $(1-\lambda_p x)^t$. Separating out the terms with $i = p$ and using the fact that $C_p^{(t+1)} = \cdots = C_p^{(d_p)} = 0$, we see that

$$\sum_{j=1}^{t} C_p^{(j)} (1-\lambda_p x)^{t-j} + \sum_{i \neq p} \sum_{j=1}^{d_i} C_i^{(j)} \frac{(1-\lambda_p x)^t}{(1-\lambda_i x)^j} = 0.$$

The left-hand side of this equation is a rational function of the variable $x$ which does not have a pole at the point $x = 1/\lambda_p$, so we can substitute this value for $x$. But every term has a factor of $(1-\lambda_p x)$ except for the term with $i = p$ and $j = t$. Thus, this equation becomes

$$C_p^{(t)} = 0$$

after substituting the value $x = 1/\lambda_p$. But this contradicts our choice of $p$ and $t$. This contradiction shows that all the coefficients $C_i^{(j)}$ in equation 4.1 must be zero, and it follows that $\mathcal{B}$ is linearly independent.

Since $\mathcal{B}$ is a set of $d$ linearly independent vectors in a vector space $\mathcal{V}_Q$ of dimension at most $d$, it follows that $\mathcal{B}$ is a basis for $\mathcal{V}_Q$, and the proof is complete. ■

▪ **Example 4.6** Let's re-examine the generating function

$$G(x) = \frac{2+5x}{1-3x^2-2x^3}$$

from Example 4.2. This satisfies the hypotheses of the Partial Fractions Theorem. The denominator $1-3x^2-2x^3$ vanishes when $x = -1$, so that $1+x$ is a factor. Some calculation shows that

$$1-3x^2-2x^3 = (1+x)(1-x-2x^2) = (1+x)^2(1-2x).$$

By the Partial Fractions Theorem, there are complex numbers $A, B, C$ such that

$$\frac{2+5x}{1-3x^2-2x^3} = \frac{A}{1+x} + \frac{B}{(1+x)^2} + \frac{C}{1-2x}.$$

Now multiply by the denominator on the LHS.

$$2+5x = A(1+x)(1-2x) + B(1-2x) + C(1+x)^2.$$

This is an equality of polynomials, so it holds for any value of $x$.

- At $x = -1$ we find that $2-5 = B(1+2)$, so that $B = -1$.
- At $x = 1/2$ we find that $2+5/2 = C(3/2)^2$, so that $9/2 = C(9/4)$, so that $C = 2$.
- At $x = 0$ we find that $2 = A+B+C$, so that $A = 2-B-C = 2+1-2 = 1$.

Therefore

$$\frac{2+5x}{1-3x^2-2x^3} = \frac{1}{1+x} - \frac{1}{(1+x)^2} + \frac{2}{1-2x}.$$

Now we can expand each of these terms using Binomial Series, and collect the results.

$$\begin{aligned} G(x) &= \sum_{n=0}^{\infty}(-x)^n - \sum_{n=0}^{\infty}\binom{n+1}{1}(-x)^n + 2\sum_{n=0}^{\infty}(2x)^n \\ &= \sum_{n=0}^{\infty}\left((-1)^n - (n+1)(-1)^n + 2\cdot 2^n\right)x^n \\ &= \sum_{n=0}^{\infty}\left(2^{n+1} - n(-1)^n\right)x^n. \end{aligned}$$

It follows that $g_n = [x^n]G(x) = 2^{n+1} + n(-1)^{n+1}$ for all $n \in \mathbb{N}$. This can be "reality checked" by comparison with the initial conditions $g_0 = 2$, $g_1 = 5$, and $g_2 = 6$, and the recurrence relation $g_n - 3g_{n-2} - 2g_{n-3} = 0$ for all $n \geq 3$ defining this sequence in Example 4.2. The first few values are

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $g_n$ | 2 | 5 | 6 | 19 | 28 | 69 | 122 |

■

## 4.4 The Main Theorem.

**Theorem 4.4.1** Let $\mathbf{g} = (g_0, g_1, g_2)$ be a sequence of integers, and let $G(x) = \sum_{n=0}^{\infty} g_n x^n$ be the corresponding generating function. Assume that the equivalent conditions of Theorem 4.2.1 hold, and that

$$G(x) = R(x) + \frac{P(x)}{Q(x)}$$

for some polynomials $P(x)$, $Q(x)$, and $R(x)$ with $\deg P(x) < \deg Q(x)$ and $Q(0) = 1$. Factor $Q(x)$ to obtain its inverse roots and their multiplicities:

$$Q(x) = (1-\lambda_1 x)^{d_1}(1-\lambda_2 x)^{d_2}\cdots(1-\lambda_s x)^{d_s}.$$

Then there are polynomials $p_i(n)$ for $1 \leq i \leq s$, with $\deg p_i(n) < d_i$, such that for all $n > \deg R(x)$,

$$g_n = p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \cdots + p_s(n)\lambda_s^n.$$

*Proof.* The conclusion of the theorem only concerns terms with $n > \deg R(x)$, so we can basically ignore the polynomial $R(x)$. In truth, all it is doing is getting in the way, and preventing the formula from holding for smaller values of $n$. So we are going to concentrate on the quotient $P(x)/Q(x)$, to which the Partial Fractions Theorem 4.3.1 applies.

Consider the factor $(1-\lambda_i x)^{d_i}$ of the denominator $Q(x)$. In the partial fractions expansion of $P(x)/Q(x)$, this contributes

$$\frac{C_i^{(1)}}{1-\lambda_i x} + \frac{C_i^{(2)}}{(1-\lambda_i x)^2} + \cdots + \frac{C_i^{(d_i)}}{(1-\lambda_i x)^{d_i}}.$$

Each term is a binomial series, and can be expanded accordingly:

$$\begin{aligned}\sum_{j=1}^{d_i} \frac{C_i^{(j)}}{(1-\lambda_i x)^j} &= \sum_{j=1}^{d_i} C_i^{(j)} \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} \lambda_i^n x^n \\ &= \sum_{n=0}^{\infty} \left( \sum_{j=1}^{d_i} C_i^{(j)} \binom{n+j-1}{j-1} \right) \lambda_i^n x^n.\end{aligned}$$

Notice that $\binom{n+j-1}{j-1}$ is a polynomial function of $n$ of degree $j-1$. It follows that

$$p_i(n) = \sum_{j=1}^{d_i} C_i^{(j)} \binom{n+j-1}{j-1}$$

is a polynomial function of $n$ of degree at most $d_i - 1$. The contribution of the inverse root $\lambda_i$ to the coefficient $g_n = [x^n]G(x)$ is thus $p_i(n)\lambda_i^n$. By the form of the partial fractions expansion we see that

$$g_n = p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \cdots + p_s(n)\lambda_s^n,$$

completing the proof. ■

The converse of Theorem 4.4.1 also holds – see Exercise 4.1.

One can use Theorem 4.4.1 to go straight from a recurrence relation to a formula for its entries, without doing Partial Fractions explicitly. Here is an example of this kind of calculation.

■ **Example 4.7** *A sequence* **h** *of integers is given by the initial conditions* $h_0 = 1$, $h_1 = 1$, $h_2 = 0$, $h_3 = 2$, $h_4 = -4$, $h_5 = 3$, *and the recurrence* $h_n - 3h_{n-1} + 4h_{n-3} = 0$ *for all* $n \geq 6$. *Obtain a formula for* $h_n$ *as a function of n.*

From Theorem 4.2.1 we see that the denominator of the generating function $H(x) = h_n x^n$ is $1 - 3x + 4x^3$. This vanishes at $x = -1$, so $1 + x$ is a factor. After some work, we obtain

$$1 - 3x + 4x^3 = (1+x)(1-4x+4x^2) = (1-2x)^2(1+x).$$

Theorem 4.4.1 implies that there are constants $A, B, C$ such that for sufficiently large $n$, $h_n = (A + Bn)2^n + C(-1)^n$. To determine these constants we need to take data from the sequence **h** from a point later than the degree of the polynomial $R(x)$ appearing in Theorem 4.4.1. From Theorem 4.2.1, in this case the degree of the numerator of the generating function $H(x)$ is no more than five, since the general case of the recurrence holds for $n \geq 6$. Writing

$$H(x) = R(x) + \frac{P(x)}{1 - 3x + 4x^3} = \frac{(1 - 3x + 4x^3)R(x) + P(x)}{1 - 3x + 4x^3},$$

it follows that the degree of $R(x)$ is at most two. So we can fit the form $h_n = (A + Bn)2^n + C(-1)^n$ to the data $h_3 = 2$, $h_4 = -4$, and $h_5 = 3$. This gives three equations in three unknowns – a standard linear algebra problem.

$$\begin{aligned} h_3 = 2 &= (A+3B)8 - C = 8A + 24B - C \\ h_4 = -4 &= (A+4B)16 + C = 16A + 64B + C \\ h_5 = 3 &= (A+5B)32 - C = 32A + 160B - C \end{aligned}$$

In this case, a grungy linear algebra problem. Sparing you the details, the solution is $A = -5/16$, $B = 1/16$, $C = -3$, and so

$$h_n = (n-5)2^{n-4} - 3(-1)^n$$

for all $n \geq 3$. The values for $h_n$ with $0 \leq n \leq 2$ are given in the initial conditions. ∎

## 4.5 Exercises.

**Exercise 4.1** Show that the converse of Theorem 4.4.1 holds. That is, assume that

$$g_n = p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \cdots + p_s(n)\lambda_s^n$$

for all $n \geq N$, in which $p_i(n)$ is a polynomial of degree strictly less than $d_i$ and the $\lambda_i$ are distinct nonzero complex numbers, for $1 \leq i \leq s$. Let

$$Q(x) = (1-\lambda_1 x)^{d_1}(1-\lambda_2 x)^{d_2}\cdots(1-\lambda_s x)^{d_s}.$$

Then

$$G(x) = \sum_{n=0}^{\infty} g_n x^n = R(x) + \frac{P(x)}{Q(x)}$$

in which $P(x)$ and $R(x)$ are polynomials, and $\deg P(x) < \deg Q(x)$ and $\deg R(x) < N$. ∎

# 5. Binary Strings.

**Definition 5.0.1** A *binary string* is a finite sequence $\sigma = b_1 b_2 \cdots b_n$ in which each *bit* $b_i$ is either 0 or 1. The number of bits is the *length* of the string, denoted $\ell(\sigma) = n$. Thus, a binary string of length $n$ is an element of the Cartesian power $\{0,1\}^n$. A binary string of arbitrary length is an element of the set $\{0,1\}^* = \bigcup_{n=0}^{\infty} \{0,1\}^n$. There is exactly one binary string $\varepsilon$ of length zero, the empty string with no bits.

Clearly, there are $2^n$ binary strings of length $n$, so that the generating function for binary strings with respect to length is

$$\Phi^{\ell}_{\{0,1\}^*}(x) = \sum_{n=0}^{\infty} 2^n x^n = \frac{1}{1-2x}.$$

In this chapter we will see how to describe various subsets of binary strings in a way which allows us to determine their generating functions with respect to length. Then the results of Chapter 4 can be applied to determine the coefficients of these power series, and thus the number of strings of a given length in such sets.

## 5.1 Regular Expressions and Rational Languages.

**Definition 5.1.1 — Regular Expressions..** A *regular expression* is defined recursively, as follows.

- All of $\varepsilon$, 0, and 1 are regular expressions.
- If R and S are regular expressions, then $\mathsf{R} \smile \mathsf{S}$ is a regular expression.
- If R and S are regular expressions, then RS is a regular expression. For any finite $k \in \mathbb{N}$ we can also use $\mathsf{R}^k$ for the $k$-fold iteration of R: that is $\mathcal{R}^2 = \mathsf{RR}$ and $\mathsf{R}^3 = \mathsf{RRR}$, and so on.
- If R is a regular expression, then $\mathsf{R}^*$ is a regular expression.

These regular expressions are just formal constructions with no intrinsic meaning. However, we will interpret them in two different ways.

- A regular expression R will *produce* a subset $\mathcal{R}$ of $\{0,1\}^*$. Such a subset is called a *rational language*.
- A regular expression R will *lead to* a rational function $R(x)$.

In general, the rational function $R(x)$ is quite meaningless. However, under favourable conditions on R, it turns out that $R(x) = \Phi^{\ell}_{\mathcal{R}}(x)$ is the generating function of $\mathcal{R}$ with respect to length. Then the machinery of Chaptere4 can be applied.

**Definition 5.1.2 — Concatenation Product.** Let $\alpha, \beta \in \{0,1\}^*$ be binary strings. Say $\alpha = a_1 a_2 \cdots a_m$ and $\beta = b_1 b_2 \cdots b_n$. The *concatenation* of $\alpha$ and $\beta$ is the string

$$\alpha\beta = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n.$$

Let $\mathcal{A}, \mathcal{B} \subseteq \{0,1\}^*$ be sets of binary strings. The *concatenation product* $\mathcal{AB}$ is the set

$$\mathcal{AB} = \{\alpha\beta : \ \alpha \in \mathcal{A} \text{ and } \beta \in \mathcal{B}\}.$$

■ **Example 5.1** Consider the sets $\mathcal{A} = \{011, 01\}$ and $\mathcal{B} = \{101, 1101\}$. There are four ways to concatenate a string in $\mathcal{A}$ followed by a string in $\mathcal{B}$:

$$011.101,\ 011.1101,\ 01.101,\ 01.1101.$$

Here, the dot . indicates the point at which the concatenation takes place. However, this information is not recorded when passing from $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$ to their concatenation $\alpha\beta$. Thus the concatenation product $\mathcal{AB}$ consists of the strings

$$011101,\ 0111101,\ 01101,\ 011101.$$

The string 011101 is produced twice. The concatenation product $\mathcal{AB}$ has only three elements:

$$\mathcal{AB} = \{011101, 0111101, 01101\}.$$

■

**Definition 5.1.3 — Rational Languages..** A *rational language* is a set $\mathcal{R} \subseteq \{0,1\}^*$ of binary strings that can be described by a regular expression. The translation of a regular expression R into a rational language $\mathcal{R}$ is denoted by $\mathsf{R} \rhd \mathcal{R}$, and is defined recursively as follows. We say that R *produces* $\mathcal{R}$. A rational language can be produced by many different regular expressions.

- To begin with, $\varepsilon \rhd \{\varepsilon\}$ and $0 \rhd \{0\}$ and $1 \rhd \{1\}$.
- If $\mathsf{R} \rhd \mathcal{R}$ and $\mathsf{S} \rhd \mathcal{S}$, then $(\mathsf{R} \smile \mathsf{S}) \rhd (\mathcal{R} \cup \mathcal{S})$.
- If $\mathsf{R} \rhd \mathcal{R}$ and $\mathsf{S} \rhd \mathcal{S}$, then $\mathsf{RS} \rhd \mathcal{RS}$. Here, $\mathcal{RS}$ is the concatenation product of $\mathcal{R}$ and $\mathcal{S}$.
- If $\mathsf{R} \rhd \mathcal{R}$ then $\mathsf{R}^* \rhd \mathcal{R}^* = \bigcup_{k=0}^{\infty} \mathcal{R}^k$. Here $\mathcal{R}^k$ is the concatenation product of $k$ copies of $\mathcal{R}$. This is called *repetition*.

In Definition 5.1.3, when $\mathsf{R} \rhd \mathcal{R}$ and $\mathsf{S} \rhd \mathcal{S}$, it might happen that $(\mathsf{R} \smile \mathsf{S}) \rhd (\mathcal{R} \cup \mathcal{S})$ is not a disjoint union of sets. Also, the concatenation product is not the same as the Cartesian product, as Example 5.1 shows.

■ **Example 5.2**

- The regular expression $1^*$ produces the rational language

$$\{1\}^* = \{\varepsilon, 1, 11, 111, 1111, ....\}$$

of all finite strings of 1s (including the empty string $\varepsilon$).
- The regular expression $(1 \smile 11)^*$ also produces the rational language $\{1\}^*$.
- The regular expression $1(11)^*$ produces the rational language consisting of all strings of 1s of odd (positive) length:

$$\{1, 111, 11111, ...\}.$$

This can be seen by working "outwards" in the regular expression. First $11 \triangleright \{1\}\{1\} = \{11\}$ by concatenation, then

$$(11)^* \triangleright \{11\}^* = \{\varepsilon, 11, 1111, ...\}$$

by repetition, and finally

$$1(11)^* \triangleright \{1\}\{\varepsilon, 11, 1111, ...\} = \{1, 111, 11111, ...\}$$

by concatenation again.
- The regular expression $(0 \smile 1)^*$ produces the rational language $\{0,1\}^*$ of all binary strings.
- The regular expression $1^*(01^*)^*$ also produces the rational language $\{0,1\}^*$ of all binary strings.

■

■ **Example 5.3**

- The regular expression $(01)^*$ produces the rational language

$$\{\varepsilon, 01, 0101, 010101, 01010101, ...\}.$$

For every even natural number $2j$ there is exactly one string of length $2j$ in this set.
- The set

$$\{\varepsilon, 01, 0011, 000111, 00001111, ...\}$$

is not a rational language, but for every even natural number $2j$ there is exactly one string of length $2j$ in this set.

■

The problem with Example 5.3 is that to describe the second set we need an expression like

$$\bigcup_{j=0}^{\infty} 0^j 1^j.$$

But this is not a regular expression. The underlying difficulty is that a regular expression has a "finite memory" and cannot remember arbitrarily large numbers, like the $j \in \mathbb{N}$ in the above expression. In fact, there is a close connection between rational languages and finite state machines, which is a central topic in the theory of computation.

## 5.2 Unambiguous Expressions and Block Decompositions.

**Definition 5.2.1 — Unambiguous Expression.** Let R be a regular expression that produces a rational language $\mathcal{R}$. Then R is *unambiguous* if every string in $\mathcal{R}$ is produced exactly once by R. If an expression is not unambiguous then it is *ambiguous*.

As usual with regular expressions, deciding whether or not it is unambiguous can be done recursively.

**Lemma 5.2.1 — Unambiguous Expression.** Let R and S be unambiguous expressions producing $\mathcal{R}$ and $\mathcal{S}$, respectively.

- All of $\varepsilon$ and 0 and 1 are unambiguous.
- The expression $\mathsf{R} \smile \mathsf{S}$ is unambiguous if and only if $\mathcal{R} \cap \mathcal{S} = \varnothing$, so that $\mathcal{R} \cup \mathcal{S}$ is a disjoint union of sets.
- The expression RS is unambiguous if and only if there is a bijection $\mathcal{RS} \rightleftharpoons \mathcal{R} \times \mathcal{S}$ between the concatenation product $\mathcal{RS}$ and the Cartesian product $\mathcal{R} \times \mathcal{S}$. In other words, for every string $\alpha \in \mathcal{RS}$ there is exactly one way to write $\alpha = \rho\sigma$ with $\rho \in \mathcal{R}$ and $\sigma \in \mathcal{S}$.
- The expression $\mathsf{R}^*$ is unambiguous if and only if each of the concatenation products $\mathcal{R}^k$ is unambiguous and the union $\bigcup_{k=0}^{\infty} \mathcal{R}^k$ is a disjoint union of sets.

The proof is left as an exercise.

■ **Example 5.4**

- The expression $1^*$ is unambiguous.
- The expression $(1 \smile 11)^*$ is ambiguous: $1.11 = 11.1 = 1.1.1$.
- The expression $(0 \smile 1)^*$ is unambiguous. This expression produces each string in $\{0,1\}^*$ one bit at a time, so each string is produced in exactly one way.
- The expression $1^*(01^*)^*$ is also unambiguous. First, the expression $01^*$ is unambiguous, since it produces a 0 follows by a (possibly empty) string of 1s – each such string is produced exactly once. Now $(01^*)^k$ is unambiguous for any $k \in \mathbb{N}$, since any string produced will begin with a 0, there will be $k$ bits equal to 0, and the strings of 1s following these 0s can only be constructed in one way. Next, $(01^*)^*$ is unambiguous, since strings produced by $(01^*)^k$ have exactly $k$ 0s for each $k \in \mathbb{N}$. Finally, $1^*(01^*)*$ is unambiguous since for any string it produces, the length of the initial sequence of 1s is determined.

■

**Definition 5.2.2 — Blocks of a string.** Let $\sigma = b_1 b_2 b_3 \cdots b_n$ be a binary string of length $n$. A *block* of $\sigma$ is a nonempty maximal subsequence of consecutive equal bits. To be clearer, that is a subsequence $b_i b_{i+1} \cdots b_j$ of consecutive bits all of which are the same (all are 0, or all are 1), which cannot be made longer. So, either $i = 1$ or $b_{i-1} \neq b_i$, and either $j = n$ or $b_{j+1} \neq b_j$.

■ **Example 5.5** The blocks of the string 111010011010011010111101 are separated by dots here:

$$111.0.1.00.11.0.1.00.11.0.1.0.111.0.1$$

■

**Proposition 5.2.2 — Block Decompositions..** The regular expressions $0^*(1^*10^*0)^*1^*$ and $1^*(0^*01^*1)^*0^*$ are unambiguous expressions for the set $\{0,1\}^*$ of all binary strings.

They produce each binary string block by block.

*Proof sketch.* By symmetry it is enough to consider the first expression. The middle part $1^*10^*0$ produces a block of 1s followed by a block of 0s. This concatenation is unambiguous. The repetition of this $(1^*10^*0)^*$ is also unambiguous, since each pass through the repetition starts with a 1 and ends with a 0. Try it out on Example 5.5. But the string we want to build might start with a block of 0s: the initial $0^*$ allows this but does not require it, since $0^* = \varepsilon \cup 0^*0$. The final $1^*$ similarly allows the string to end with a block of 1s, but does not require it. All the operations are unambiguous, so the whole expression is unambiguous. ■

## 5.3 Translation into Generating Functions.

**Definition 5.3.1** Let $\mathcal{R}$ be a regular expression. We translate $\mathcal{R}$ into a rational function $R(x)$ as follows using the notation $\mathcal{R} \rightsquigarrow R(x)$ and terminology $\mathcal{R}$ *leads to* $R(x)$. The definition is recursive. Assume that $\mathcal{R}$ and $\mathcal{S}$ are regular expressions such that $\mathcal{R} \rightsquigarrow R(x)$ and $\mathcal{S} \rightsquigarrow S(x)$.

- To begin with, $\varepsilon \rightsquigarrow 1$ and $0 \rightsquigarrow x$ and $1 \rightsquigarrow x$.
- The expression $\mathcal{R} \cup \mathcal{S}$ leads to $R(x) + S(x)$.
- The expression $\mathcal{RS}$ leads to $R(x)S(x)$.
- The expression $\mathcal{R}^*$ leads to $1/(1-R(x))$.

▪ **Example 5.6**

- The unambiguous expression $1^*$ leads to $1/(1-x)$.
- The ambiguous expression $(1 \cup 11)^*$ leads to $1/(1-(x+x^2))$. But this expression produces the same rational language as $1^*$.
- The unambiguous expression $(0 \cup 1)^*$ leads to $1/(1-(x+x)) = 1/(1-2x)$.
- The unambigous expression $1^*(01^*)^*$ leads to

$$\left(\frac{1}{1-x}\right)\frac{1}{1-x(\frac{1}{1-x})} = \frac{1}{1-2x}.$$

▪

**Theorem 5.3.1** Let $\mathcal{R}$ be a regular expression producing the rational language $\mathcal{L}$, and let $\mathcal{R} \rightsquigarrow R(x)$ as in Definition 5.3.1. If $\mathcal{R}$ is an unambiguous expression for $\mathcal{L}$ then $R(x) = \Phi^{\ell}_{\mathcal{L}}(x)$, the generating function for $\mathcal{L}$ with respect to length.

*Proof.* The proof of this is by induction on the complexity of the expression, using the fact that it is unambiguous. Certainly, each of $\varepsilon$, 0, and 1 are unambiguous, leading to the correct generating functions for the sets $\{\varepsilon\}$, $\{0\}$, and $\{1\}$, respectively. The remaining cases follow from the Sum Lemma, Product Lemma, and String Lemma, respectively, because each of the operations is unambiguous. ■

▪ **Example 5.7** If the regular expression $\mathcal{R}$ producing $\mathcal{L}$ is ambiguous, then the rational function $R(x)$ is in general meaningless. For example, consider the regular expression $(\varepsilon \cup 1)^*$, which produces the rational language $\{1\}^*$. It is an ambiguous expression. (In fact, every string of 1s is produced infinitely many times.) The generating function for $\{1\}^*$

with respect to length is $1/(1-x)$. The expression $(\varepsilon \smile 1)^*$ leads to $1/(1-(1+x)) = -x^{-1}$. This isn't even a power series. If it were a generating function it would say that there are exactly $-1$ things of size $-1$, and nothing else. This makes no sense.

Similarly, the ambiguous expression $(1 \smile 11)^*$ produces the set $\{1\}^*$, which has generating function $1/(1-x)$. However the expression $(1 \smile 11)^*$ leads to $1/(1-x-x^2)$ which is incorrect. ∎

∎ **Example 5.8** The block decomposition $0^*(1*10*0)^*1^*$ is unambiguous, and produces $\{0,1\}^*$. It had better lead to the right generating function! After a bit of calculation, we get

$$\frac{1}{1-x} \cdot \frac{1}{1-\left(\frac{x}{1-x}\right)^2} \cdot \frac{1}{1-x} = \frac{1}{1-2x},$$

which is good. ∎

This technique is very well-suited to enumerating sets of binary strings which are determined by conditions on the lengths of their blocks. It can also be used to enumerate sets of strings which avoid some particular substring or strings. Here are a few examples.

∎ **Example 5.9** Let $\mathcal{L}$ be the set of binary strings in which every block of 1s has odd length. What is the generating function for $\mathcal{L}$ with respect to length? Consider the block decomposition $0^*(1^*10^*0)^*1^*$ for all binary strings. The expression $1^*1$ in the middle produces a block of 1s. The expression $1^* \approx \varepsilon \smile 1^*1$ produces either the empty string or a block of 1s. If we want a block of 1s of odd length, then that is produced by $(11)^*1$. So the expression

$$0^*((11)^*10^*0)^*(\varepsilon \smile (11)^*1)$$

is a block decomposition for the set $\mathcal{L}$ in question. It is therefore an unambiguous expression. This expression leads to

$$\begin{aligned}\Phi^{\ell}_{\mathcal{L}}(x) &= \frac{1}{1-x} \cdot \frac{1}{1-\left(\frac{x}{1-x^2}\right)\left(\frac{x}{1-x}\right)} \cdot \left(1+\frac{x}{1-x^2}\right) \\ &= \frac{1+x-x^2}{(1-x)(1-x^2)-x^2} = \frac{1+x-x^2}{1-x-2x^2+x^3}.\end{aligned}$$

It follows that the number $g_n$ of strings of length $n$ in $\mathcal{L}$ satisfies the linear recurrence relation with initial conditions such that

$$g_n - g_{n-1} - 2g_{n-2} + g_{n-3} = \begin{cases} 1 & \text{if } n=0, \\ 1 & \text{if } n=1, \\ -1 & \text{if } n=2, \\ 0 & \text{if } n \geq 3, \end{cases}$$

with the convention that $g_n = 0$ for all $n < 0$. This gives the inital conditions $g_0 = 1$, $g_1 = 2$, $g_2 = 3$, and the recurrence $g_n = g_{n-1} + 2g_{n-2} - g_{n-3}$ for all $n \geq 3$. It is easy to calculate the first several of these numbers.

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $g_n$ | 1 | 2 | 3 | 6 | 10 | 19 | 33 | 61 | 108 |

To get an exact formula for $g_n$ we would need to factor the denominator $1-x-2x^2+x^3$ to find its inverse roots. They turn out to be really horrible complex numbers, so we won't do it. ∎

■ **Example 5.10** Let $\mathcal{L}$ be the set of binary strings that do not contain 0011 as a substring. By this we mean that the bits 0011 cannot occur as a sequence of consecutive bits in a string in $\mathcal{L}$. To get an unambiguous expression that produces $\mathcal{L}$, it is sensible to consider the block decomposition $1^*(0^*01^*1)^*0^*$, since the middle part $0^*01^*1$ produces a block of 0s followed by a block of 1s. Avoiding 0011 as a substring means that if a block of at least two 0s is followed by a block of 1s, then that block of 1s has length one. This is produced by the regular expression $01^*1 \smile 0^*001$, and this is unambiguous. It follows that

$$1^*(01^*1 \smile 0^*001)^*0^*$$

is a block decomposition for $\mathcal{L}$. This leads to the generating function

$$\begin{aligned}\Phi^{\ell}_{\mathcal{L}}(x) &= \frac{1}{1-x}\cdot\frac{1}{1-\left(\frac{x^2}{1-x}+\frac{x^3}{1-x}\right)}\cdot\frac{1}{1-x}\\ &= \frac{1}{(1-x)^2-(x^2+x^3)(1-x)} = \frac{1}{1-2x+x^4}.\end{aligned}$$

■

■ **Example 5.11** ■

## 5.4 Exercises.

**Exercise 5.1** Let $\mathcal{L}$ be the set of binary strings that do not contain 0001 as a substring. Show that the generating function for $\mathcal{L}$ is

$$\frac{1}{1-2x+x^4}.$$

■

**Exercise 5.2** Let $\mathcal{L}$ be the set of binary strings that do not contain 00111 as a substring. Show that the generating function for $\mathcal{L}$ is

$$\frac{1}{1-2x+x^5}.$$

■

**Exercise 5.3** Let $a \geq 1$ and $b \geq 1$ be positive integers, and let $\mathcal{L}$ be the set of binary strings that do not contain $0^a1^b$ as a substring. Show that the generating function for $\mathcal{L}$ is

$$\frac{1}{1-2x+x^{a+b}}.$$

■

**Exercise 5.4** Let $\mathcal{L}$ be the set of binary strings that do not contain 0101 as a substring. Obtain a formula for the generating function for $\mathcal{L}$. (Hint: consider an expression $(01\mathcal{R})^*$, in which $\mathcal{R}$ is an unambiguous expression that produces all **nonempty** strings that do not contain 01 as a substring.) ■

**Exercise 5.5** Let $\mathcal{L}$ be the set of binary strings that do not contain 010101 as a substring. Obtain a formula for the generating function for $\mathcal{L}$. ■

**Exercise 5.6** ■

# 6. Computing Averages.

## 6.1 Bivariate Generating Functions.

So far we have been dealing with power series $G(x)$ in one variable. In many cases this is a generating function for some set with respect to some statistic. For example, for $t \in \mathbb{N}$, $1/(1-x)^t$ is the generating function for multisets with $t$ types of element, enumerated with respect to size. A power series with one variable can keep track of one piece of information in the exponent of that variable. To keep track of two pieces of information we need two variables.

**Definition 6.1.1** Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$. Let $f : \mathcal{A} \to \mathbb{N}$ be any other function. The *bivariate generating function* determined by this information is

$$\Phi_{\mathcal{A}}^{\omega,f}(x,y) = \sum_{\alpha \in \mathcal{A}} x^{\omega(\alpha)} y^{f(\alpha)}.$$

We can collect like powers of $x$ and write this in the form

$$\Phi_{\mathcal{A}}^{\omega,f}(x,y) = \sum_{n=0}^{\infty} a_n(y) x^n$$

in which

$$a_n(y) = \sum_{\alpha \in \mathcal{A}:\ \omega(\alpha)=n} y^{f(\alpha)}.$$

Notice that since $\omega$ is a weight function, each of the $a_n(y)$ is a finite sum, and so is a polynomial in the variable $y$ with nonnegative integer coefficients. Also notice that if we set $y = 1$ then we get the result of Proposition **??**: $[x^n]\Phi_{\mathcal{A}}(x,1) = a_n(1)$ is the number of elements in $\mathcal{A}$ of weight $n$. So this bivariate generating function is a power series in $x$ with coefficients that are polynomials in $y$. This allows us to calculate with them as power series in $x$ without getting into trouble. We'll see how to use this shortly.

The Sum Lemma, Product Lemma, and String Lemma continue to hold in this generality. The proofs are left as exercises.

**Lemma 6.1.1 — The Sum Lemma..** Let $\mathcal{A}$ and $\mathcal{B}$ be disjoint sets, so that $\mathcal{A}\cap\mathcal{B}=\varnothing$. Assume that $\omega:(\mathcal{A}\cup\mathcal{B})\to\mathbb{N}$ is a weight function on the union of $\mathcal{A}$ and $\mathcal{B}$. We may regard $\omega$ as a weight function on each of $\mathcal{A}$ or $\mathcal{B}$ separately (by restriction). Also, let $f:(\mathcal{A}\cup\mathcal{B})\to\mathbb{N}$ be any other function. Under these conditions,

$$\Phi^{\omega,f}_{\mathcal{A}\cup\mathcal{B}}(x,y)=\Phi^{\omega,f}_{\mathcal{A}}(x,y)+\Phi^{\omega,f}_{\mathcal{B}}(x,y).$$

**Lemma 6.1.2 — The Product Lemma..** Let $\mathcal{A}$ and $\mathcal{B}$ be sets with weight functions $\omega:\mathcal{A}\to\mathbb{N}$ and $\nu:\mathcal{B}\to\mathbb{N}$, respectively. Let $f:\mathcal{A}\to\mathbb{N}$ and $g:\mathcal{B}\to\mathbb{N}$ be any functioins. Define $\theta:\mathcal{A}\times\mathcal{B}\to\mathbb{N}$ by putting $\theta(\alpha,\beta)=\omega(\alpha)+\nu(\beta)$ for all $(\alpha,\beta)\in\mathcal{A}\times\mathcal{B}$. Define $h:\mathcal{A}\times\mathcal{B}\to\mathbb{N}$ by putting $h(\alpha,\beta)=f(\alpha)+g(\beta)$ for all $(\alpha,\beta)\in\mathcal{A}\times\mathcal{B}$. Then $\theta$ is a weight function on $\mathcal{A}\times\mathcal{B}$ and

$$\Phi^{(\theta,h)}_{\mathcal{A}\times\mathcal{B}}(x,y)=\Phi^{\omega,f)}_{\mathcal{A}}(x,y)\cdot\Phi^{\nu,g}_{\mathcal{B}}(x,y).$$

**Lemma 6.1.3 — The String Lemma..** Let $\mathcal{A}$ be a set with a weight function $\omega:\mathcal{A}\to\mathbb{N}$ such that there are no elements of $\mathcal{A}$ of weight zero. Let $f:\mathcal{A}\to\mathbb{N}$ be any otjher function. Then

$$\Phi^{\omega^*,f^*}_{\mathcal{A}^*}(x,y)=\frac{1}{1-\Phi^{\omega,f}_{\mathcal{A}}(x,y)}.$$

■ **Example 6.1** Consider the set $\mathcal{C}=\mathbb{P}^*$ of all compositions, enumerated with respect to both size and length. That is,

$$\Phi_{\mathcal{C}}(x,y)=\sum_{\gamma\in\mathbb{P}^*}x^{|\gamma|}y^{\ell(\gamma)}.$$

In this expression, for a composition $\gamma=(c_1,c_2,\ldots,c_k)$ we have $|\gamma|=c_1+c_2+\cdots+c_k$ and $\ell(\gamma)=k$. Note that $|\cdot|:\mathcal{C}\to\mathbb{N}$ is a weight function, and $\ell:\mathcal{C}\to\mathbb{N}$ is some other function.

- A single part $c$ contributes $x^cy$, and since $c\in\mathbb{P}$ is arbitrary, a single part contributes

$$\sum_{c=1}^{\infty}x^cy=\frac{xy}{1-x}.$$

- By the Product Lemma, a composition with $k$ parts contributes

$$\left(\frac{xy}{1-x}\right)^k.$$

  (Notice that the hypotheses of the Product Lemma are satisfied.)
- Since the length $k$ is arbitrary, we conclude that

$$\Phi_{\mathcal{C}}(x,y)=\sum_{k=0}^{\infty}\left(\frac{xy}{1-x}\right)^k=1+\frac{xy}{1-x-xy},$$

by the String Lemma. Notice that if we set $y = 1$ then we obtain the formula from Example ?.?.?.

■

■ **Example 6.2** Consider the set $\mathcal{C} = \mathbb{P}^*$ of all compositions, enumerated with respect to both size and how many parts are equal to one. That is,

$$\Phi_{\mathcal{C}}(x,y) = \sum_{\gamma \in \mathbb{P}^*} x^{|\gamma|} y^{b(\gamma)}.$$

In this expression, for a composition $\gamma = (c_1, c_2, ..., c_k)$ we have $|\gamma| = c_1 + c_2 + \cdots + c_k$ and $b(\gamma) = |\{i : \ 1 \leq i \leq k \text{ and } c_i = 1\}|$.

- A single part $c$ contributes $xy$ if $c = 1$, and $x^c$ if $c \geq 2$. Since $c \in \mathbb{P}$ is arbitrary, a single part contributes
$$xy + \sum_{c=2}^{\infty} x^c = xy + \frac{x^2}{1-x}.$$
- A composition with $k$ parts contributes
$$\left( xy + \frac{x^2}{1-x} \right)^k.$$
- Since the length $k$ is arbitrary, we conclude that
$$\Phi_{\mathcal{C}}(x,y) = \sum_{k=0}^{\infty} \left( xy + \frac{x^2}{1-x} \right)^k = \frac{1-x}{1-x-xy-x^2+x^2y}.$$

Notice that if we set $y = 1$ then we obtain the formula from Example ?.?.?.

■

## 6.2 The General Formula.

**Theorem 6.2.1** Let $\mathcal{A}$ be a set with a weight function $\omega : \mathcal{A} \to \mathbb{N}$ and any other function $f : \mathcal{A} \to \mathbb{N}$. Let

$$A(x,y) = \Phi_{\mathcal{A}}^{\omega,f}(x,y) = \sum_{\alpha \in \mathcal{A}} x^{\omega(\alpha)} y^{f(\alpha)}$$

be the corresponding bivariate generating function.

1. For any $n \in \mathbb{N}$, the number of elements in $\mathcal{A}$ of weight $n$ is $[x^n]A(x,1)$.
2. For any $n \in \mathbb{N}$, the average value of $b(\alpha)$ among all $\alpha \in \mathcal{A}$ of weight $n$ is
$$\frac{1}{[x^n]A(x,1)} [x^n] \frac{\partial}{\partial y} A(x,y) \Big|_{y=1}.$$

*Proof.* This looks complicated, but it is not really hard. We have already remarked above

upon the first point. For the second point we just calculate that

$$\begin{aligned}
& [x^n]\,\frac{\partial}{\partial y}A(x,y)\Big|_{y=1} \\
= \;& [x^n]\,\frac{\partial}{\partial y}\sum_{\alpha\in\mathcal{A}} x^{\omega(\alpha)}y^{f(\alpha)}\Big|_{y=1} \\
= \;& [x^n]\sum_{\alpha\in\mathcal{A}} x^{\omega(\alpha)}f(\alpha) \\
= \;& \sum_{\alpha\in\mathcal{A}:\ \omega(\alpha)=n} f(\alpha).
\end{aligned}$$

This is the sum of $f(\alpha)$ over all $\alpha\in\mathcal{A}$ of weight $n$. Dividing by $[x^n]A(x,1)$ gives the average value of $f(\alpha)$ over all $\alpha\in\mathcal{A}$ of weight $n$, as claimed. ■

## 6.3 Examples.

■ **Example 6.3** What is the average length among all compositions of size $n$? Let us call this number $\overline{\ell}(n)$. There is one composition of size zero, and it has length zero, so $\overline{\ell}(0)=0$. For $n\geq 1$ there are $2^{n-1}$ compositions of size $n$, by Example ?.?.?. The generating function for compositions with respect to both size and length is

$$1+\frac{xy}{1-x-xy},$$

by Example ?.?.?. Applying Theorem 6.2.1, we calculate that

$$\begin{aligned}
& \frac{\partial}{\partial y}1+\frac{xy}{1-x-xy}\Big|_{y=1} \\
= \;& \frac{x}{1-2x}+\frac{x(-1)(-x)}{(1-2x)^2}=\frac{x-x^2}{(1-2x)^2} \\
= \;& \sum_{i=0}^{\infty}\binom{i+1}{1}2^i x^{i+1}-\sum_{j=0}^{\infty}\binom{j+1}{1}2^j x^{j+2} \\
= \;& \sum_{k=1}^{\infty}k2^{k-1}x^k-\sum_{k=2}^{\infty}(k-1)2^{k-2}x^k \\
= \;& x+\sum_{k=2}^{\infty}(k+1)2^{k-2}x^k.
\end{aligned}$$

Extracting the coefficient of $x^n$ from this and dividing by $2^{n-1}$, we find that

$$\overline{ell}(n)=\begin{cases} 0 & \text{if } n=0,\\ 1 & \text{if } n=1,\\ (n+1)/2 & \text{if } n\geq 2.\end{cases}$$

■

■ **Example 6.4** What is the average number of parts of size 1 among all compositions of size $n$? Let us call this number $\overline{b}(n)$. There is one composition of size zero, and it has no

parts of size 1, so $\overline{b}(0) = 0$. For $n \geq 1$ there are $2^{n-1}$ compositions of size $n$, by Example ?.?.?. The generating function for compositions with respect to both size and number of parts of size 1 is

$$\frac{1-x}{1-x-xy-x^2+x^2y},$$

by Example ?.?.?. Applying Theorem 6.2.1, we calculate that

$$\begin{aligned}
& \frac{\partial}{\partial y}\frac{1-x}{1-x-xy-x^2+x^2y}\bigg|_{y=1} \\
= \;& \frac{(1-x)(-1)(-x+x^2)}{(1-2x)^2} = \frac{x-2x^2+x^3}{(1-2x)^2} \\
= \;& \sum_{i=0}^{\infty}\binom{i+1}{1}2^i x^{i+1} - 2\sum_{j=0}^{\infty}\binom{j+1}{1}2^j x^{j+2} + \sum_{k=0}^{\infty}\binom{k+1}{1}2^k x^{k+3} \\
= \;& \sum_{k=1}^{\infty} k2^{k-1}x^k - 2\sum_{k=2}^{\infty}(k-1)2^{k-2}x^k + \sum_{k=3}^{\infty}(k-2)2^{k-3}x^k \\
= \;& x + (2\cdot 2-2)x^2 + \sum_{k=3}^{\infty}\Big(k2^{k-1} - (k-1)2^{k-1} + (k-2)2^{k-3}\Big)x^k \\
= \;& x + 2x^2 + \sum_{k=0}^{\infty}(k+2)2^{k-3}x^k,
\end{aligned}$$

after a bit of algebra. Extracting the coefficient of $x^n$ from this and dividing by $2^{n-1}$, we find that

$$\overline{b}(n) = \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ 1 & \text{if } n = 2, \\ (n+2)/4 & \text{if } n \geq 3. \end{cases}$$

As a "reality check" consider the compositions of size 4:

$$(4),\ (3,1),\ (1,3),\ (2,2),\ (2,1,1),\ (1,2,1),\ (1,1,2),\ (1,1,1,1).$$

There are a total of 12 parts of size 1 among these 8 compositions, so the average number of parts of size 1 is $\overline{b}(4) = 12/8 = 3/2 = (4+2)/4$, as above. ∎

The theory of regular expressions and rational languages of binary strings can be extended accordingly. The only new piece is how to keep track of the new statistic $f(\sigma)$ in the exponent of the second variable $y$. But as long as the Sum and Product Lemmas of Section 6.1 are verified, there are no extra difficulties.

∎ **Example 6.5** Among all $2^n$ binary strings $\sigma$ of length $n$, what is the average number of blocks of $\sigma$? Let $\{0,1\}^*$ be the set of all binary strings, and let $\ell(\sigma)$ and $b(\sigma)$ be the length and number of blocks of $\sigma$, respectively. Consider the bivariate generating function

$$B(x,y) = \sum_{\sigma\in\{0,1\}^*} x^{\ell(\sigma)}y^{b(\sigma)}.$$

We're going to analyze this, essentially by using the block decomposition $0^*(1^*10^*0)^*1^*$.

- A single block (in either $0^*0$ or $1^*1$) of length $k$ contributes $x^k y^1$, since it has length $k$ and is one block. Note that the empty string still contributes $x^0 y^0 = 1$ since it has length zero and is not a block. So the generating function for a single block is

$$\sum_{k=1}^{\infty} x^k y = \frac{xy}{1-x}.$$

  (Here we use the Sum Lemma.)
- By the Product Lemma, the generating function for a sequence of $m$ blocks is $x^m y^m/(1-x)^m$. (To see that the Product Lemma applies, check that the number of blocks $b$ is additive for blocks.)
- The "inner loop" of our block decomposition is an arbitrary repetition of two blocks at a time. By the Product Lemma, the generating function for this is $(1-x^2y^2/(1-x)^2)^{-1}$.
- Putting this all together, we have

$$B(x,y) = \left(1+\frac{xy}{1-x}\right)\frac{1}{1-(xy/(1-x)^2}\left(1+\frac{xy}{1-x}\right).$$

This can be simplified:

$$\begin{aligned} B(x,y) &= \left(\frac{1-x+xy}{1-x}\right)^2 \frac{(1-x)^2}{(1-x)^2-(xy)^2} \\ &= \frac{(1-x+xy)^2}{(1-x-xy)(1-x+xy} = \frac{1-x+xy}{1-x-xy}. \end{aligned}$$

(The second step is by difference of squares.) Note that $B(x,1) = 1/(1-2x)$, as it should be – a good reality check. Finally, we apply Theorem 6.2.1:

$$\begin{aligned} & \frac{\partial}{\partial y}\frac{1-x+xy}{1-x-xy}\bigg|_{y=1} \\ = \; & \frac{x}{1-2x} + \frac{(-1)(-x)}{(1-2x)^2} \\ = \; & x\sum_{i=0}^{\infty} 2^i x^i + x\sum_{j=0}^{\infty}(j+1)2^j x^j. \end{aligned}$$

(Here we used geometric and binomial series.) Extracting the coefficient of $x^n$ gives 0 if $n=0$, and for $n \geq 1$ it is

$$2^{n-1} + n2^{n-1} = 2^{n-1}(n+1).$$

Dividing by $2^n$, we see that the average number of blocks among all binary strings of length $n$ is 0 if $n=0$, and is $(n+1)/2$ for $n \geq 1$. This clearly works for $n=1$. Let's check for $n=3$:

$$000\ 001\ 010\ 011\ 100\ 101\ 110\ 111$$

and there are 16 blocks among 8 strings, and $16/8 = (3+1)/2$. ∎

∎ **Example 6.6** ∎

## 6.4 Exercises.

# 7. Quadratic Recursion.

## 7.1 The Binomial Series.

In Section ?.?.? we saw the Binomial Theorem and The Binomial Series with negative integer exponents. That is, for a natural number $n \in \mathbb{N}$,

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

and for a positive integer $t \geq 1$,

$$\frac{1}{(1-x)^t} = \sum_{n=0}^{\infty} \binom{n+t-1}{t-1} x^n.$$

These are two special cases of the *binomial series expansion*.

### 7.1.1 The General Case.

**Definition 7.1.1** For any complex number $\alpha \in \mathbb{C}$ and nonnegative integer $k \in \mathbb{N}$, the *k-th binomial coefficient of* $\alpha$ is

$$\binom{\alpha}{k} = \frac{1}{k!}(\alpha)(\alpha-1)\cdots(\alpha-k+1).$$

This is a polynomial function of $\alpha$ of degree $k$.

**Theorem 7.1.1** The Binomial Series. For any complex number $\alpha \in \mathbb{C}$,

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k.$$

*Proof.* We can think of $(1+x)^\alpha$ as a function of a complex variable $x$. The only possible singularity is $0^\alpha$ which might not be well-defined – this happens only for $x=-1$ Therefore, $(1+x)^\alpha$ is analytic in the disc $|x|<1$, and so it has a Taylor series expansion. By Taylor's Theorem, the coefficient of $x^k$ in this Taylor series expansion is

$$\frac{1}{k!}\frac{\mathrm{d}^k}{\mathrm{d}x^k}(1+x)^\alpha\Big|_{x=0} = \frac{1}{k!}(\alpha)(\alpha-1)\cdots(\alpha-k+1)(1+x)^{\alpha-k}\Big|_{x=0} = \binom{\alpha}{k}.$$

This proves the stated formula. ■

Two special cases if the Binomial Series will be especially important for us.

### 7.1.2 Exponent $\alpha = -1/2$.

The power series $(1-4x)^{-1/2}$ turns out to be interesting and useful. By the Binomial Series,

$$\frac{1}{\sqrt{1-4x}} = \sum_{k=0}^{\infty} \binom{-1/2}{k}(-4x)^k = \sum_{k=0}^{\infty}(-1)^k 4^k \binom{-1/2}{k} x^k.$$

Let's look at the coefficient of $x^k$ in this, for each $k \in \mathbb{N}$.

$$\begin{aligned}
(-1)^k 4^k \binom{-1/2}{k} &= (-1)^k 4^k \frac{1}{k!}(-1/2)(-3/2)(-5/2)\cdots(-1/2-k+1) \\
&= 4^k \frac{1}{k!}(1/2)(3/2)(5/2)\cdots(k-1/2) \\
&= 2^k \frac{1}{k!}(1)(3)(5)\cdots(2k-1) \\
&= \frac{1}{k!k!}(1)(2)(3)(4)(5)\cdots(2k-1)(2k) = \binom{2k}{k}.
\end{aligned}$$

In summary, we have proved the following.

**Proposition 7.1.2**

$$\frac{1}{\sqrt{1-4x}} = \sum_{k=0}^{\infty} \binom{2k}{k} x^k.$$

### 7.1.3 Exponent $\alpha = 1/2$.

The power series $(1-4x)^{1/2}$ is even more interesting and useful. By the Binomial Series,

$$\sqrt{1-4x} = \sum_{k=0}^{\infty} \binom{1/2}{k}(-4x)^k = \sum_{k=0}^{\infty}(-1)^k 4^k \binom{1/2}{k} x^k.$$

For $k=0$ the coefficient of $x^0$ is $(-1)^0 4^0 \binom{1/2}{0} = 1$. For $k \geq 1$ we can calculate as follows.

$$\begin{aligned}(-1)^k 4^k \binom{1/2}{k} &= (-1)^k 4^k \frac{1}{k!}(1/2)(-1/2)(-3/2)\cdots(1/2-k+1) \\ &= -4^k \frac{1}{k!}(1/2)(1/2)(3/2)\cdots(k-3/2) \\ &= -2^k \frac{1}{k!}(1)(1)(3)(5)\cdots(2k-3) \\ &= -2\frac{1}{k!(k-1)!}(1)(2)(3)(4)\cdots(2k-4)(2k-3)(2k-2) = \frac{-2}{k}\binom{2k-2}{k-1}.\end{aligned}$$

(It is worth checking where we needed the fact that $k \geq 1$ in this computation. In summary, se have proved the following.

**Proposition 7.1.3**

$$\sqrt{1-4x} = 1 - 2\sum_{k=1}^{\infty} \frac{1}{k}\binom{2k-2}{k-1}x^k = 1 - 2\sum_{k=0}^{\infty} \frac{1}{k+1}\binom{2k}{k}x^{k+1}.$$

The numbers $C_n = \frac{1}{n+1}\binom{2n}{n}$ are called *Catalan numbers*. The first few Catalan numbers are shown here:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_n$ | 1 | 1 | 2 | 5 | 14 | 42 | 132 | 429 | 1430 | 4862 | 16796 |

## 7.2 Quadratic Recursion.

Let $\mathbf{g} = (g_0, g_1, g_2, \ldots)$ be a sequence of numbers with generating function $G(x) = \sum_{n=0}^{\infty} g_n x^n$. In Theorem ?.? we saw that $\mathbf{g}$ satisfies a homogeneous linear recurrence relation (with initial conditions) if and only if $G(x) = P(x)/Q(x)$ is a quotient of two polynomials. Rewriting this as $Q(x)G(x) - P(x) = 0$, we see that $G(x)$ is a solution to a linear equation: $QG - P = 0$.

**Definition 7.2.1** The sequence $\mathbf{g}$ satisfies a *quadratic recurrence* if its generating function $G(x)$ satisfies a quadratic equation:

$$A(x)G(x)^2 + B(x)G(x) + C(x) = 0.$$

Here, the coefficients $A(x)$, $B(x)$, and $C(x)$ can be any power series in the variable $x$.

There are two solutions to the equation in Definition ?.?.?, and they can be found using the Quadratic Formula:

$$\left.\begin{matrix} G_+(x) \\ G_-(x) \end{matrix}\right\} = \frac{-B(x) \pm \sqrt{B(x)^2 - 4A(x)C(x)}}{2A(x)}.$$

Rigorous justification for this kind of algebra with power series is discussed in detail in CO 330. If $G(x)$ is a generating function for some combinatorial objects then it has only nonnegative coefficients and nonnegative exponents. This can be used to decide which case of the $\pm$ to take: in general, only one of $G_+(x)$ or $G_-(x)$ is the correct generating function.

■ **Example 7.1 — Well-Formed Parenthesizations..** A *well-formed parenthesization* (WFP) is a sequence of $n$ opening parentheses and $n$ closing parentheses which "match together" using the usual rules for grouping parentheses. The *size* of a WFP is the number of opening parentheses in it. Here are all the WFPs of size 3:

$$()()(),\ ()(()),\ (())(),\ (()()),\ ((())).$$

Here are all the WFPs of size 4:

$()()()()$ $(()())()$
$()()(())$ $((()))()$
$()(())()$ $(()()())$
$()(()())$ $(()(()))$
$()((()))$ $((())())$
$(())()()$ $((()()))$
$(())(())$ $(((())))$

For each $n \in \mathbb{N}$, let $w_n$ be the number of WFPs of size $n$. So $w_3 = 5$ and $w_4 = 14$. Let

$$W(x) = \sum_{n=0}^{\infty} w_n x^n$$

be the generating function for WFPs with respect to size.

We can obtain a quadratic recurrence for $W(x)$, as follows. The empty sequence $\varepsilon$ contributes $x^0 = 1$ to the generating function $W(x)$. Any other WFP $\gamma$ begins with an opening parenthesis. There is exactly one closing parenthesis which matches to the beginning parenthesis. That is, $\gamma = (\alpha)\beta$ for some other sequences $\alpha$ and $\beta$. Note that $\alpha$ or $\beta$ might be empty. Because of the way parentheses are matched to each other, both $\alpha$ and $\beta$ are in fact WFPs themselves. The total number of opening parentheses in $\gamma$ is $n(\gamma) = 1 + n(\alpha) + n(\beta)$. Conversely, given any WFPs $\alpha$ and $\beta$ we can always form a new (nonempty) WFP $(\alpha)\beta$. This allows us to calculate as follows:

$$\begin{aligned}
W(x) &= \sum_{\gamma \in \mathcal{W}} x^{n(\gamma)} \\
&= x^{n(\varepsilon)} + \sum_{\gamma \in \mathcal{W} \setminus \{\varepsilon\}} x^{n(\gamma)} \\
&= 1 + \sum_{\alpha \in \mathcal{W}} \sum_{\beta \in W} x^{1+n(\alpha)+n(\beta)} \\
&= 1 + x \left( \sum_{\alpha \in \mathcal{W}} x^{n(\alpha)} \right) \left( \sum_{\beta \in \mathcal{W}} x^{n(\beta)} \right) \\
&= 1 + xW(x)^2.
\end{aligned}$$

Now we can solve this equation $xW(x)^2 - W(x) + 1 = 0$ using the Quadratic Formula:

$$\left.\begin{matrix} W_+(x) \\ W_-(x) \end{matrix}\right\} = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

We have seen how to expand $\sqrt{1-4x}$ using the Binomial Series, so

$$\frac{1\pm\sqrt{1-4x}}{2x} = \frac{1}{2x} \pm \frac{1}{2x}\left(1 - 2\sum_{k=0}^{\infty}\frac{1}{k+1}\binom{2k}{k}x^{k+1}\right).$$

To get nonnegative coefficients, and to cancel the term $1/(2x)$, we need to take the minus sign from the $\pm$. The result is

$$W(x) = \sum_{k=0}^{\infty}\frac{1}{k+1}\binom{2k}{k}x^k,$$

so the number of WFPs of size $n$ is the $n$-th Catalan number $w_n = \frac{1}{n+1}\binom{2n}{n}$, for each $n \in \mathbb{N}$.
■

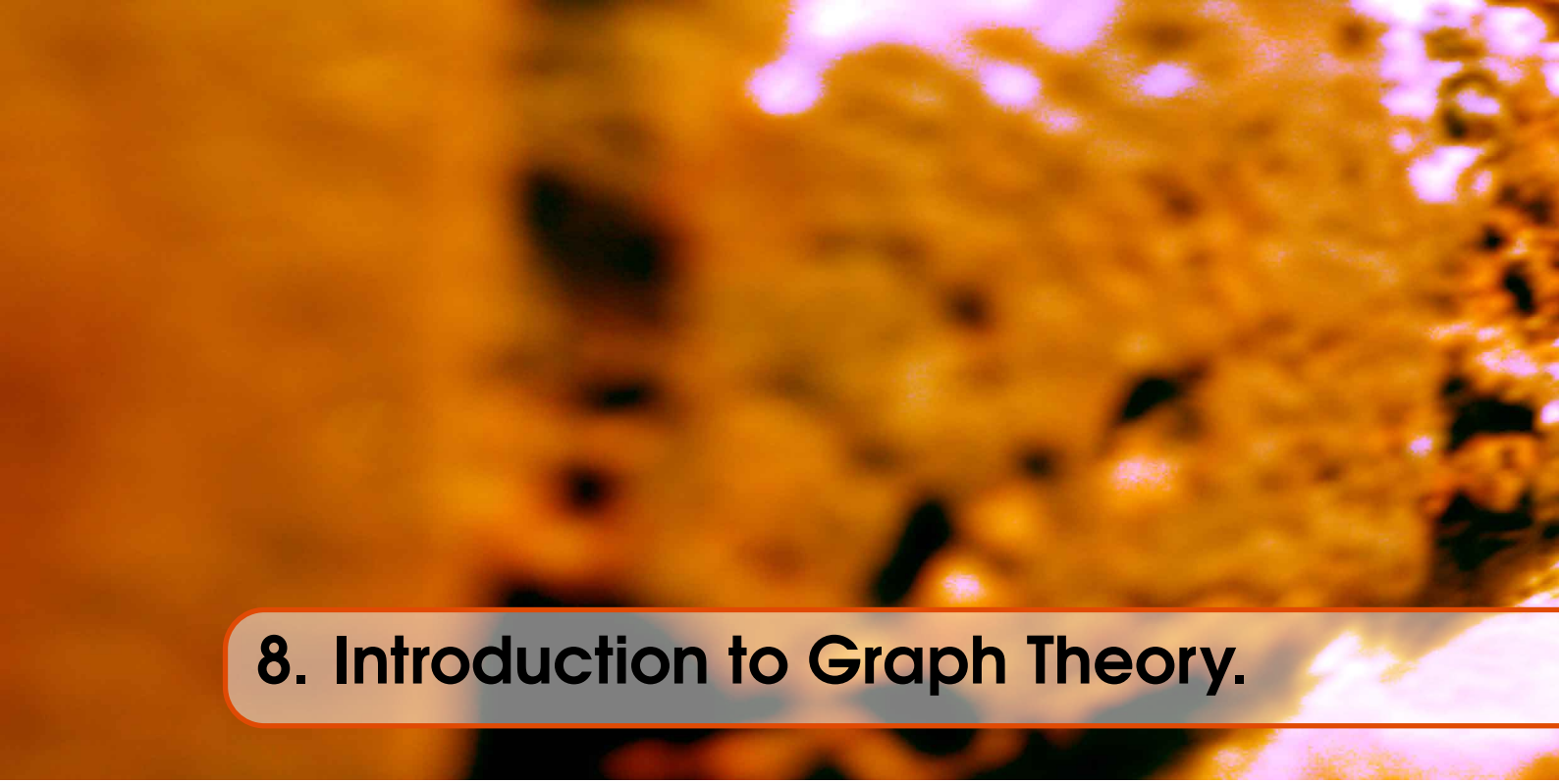
## 7.3 Exercises.

**Exercise 7.1** Consider the set $\mathcal{W}$ of well-formed parenthesizations (WFPs). For $\pi \in \mathcal{W}$, the size $n(\pi)$ is the number of closing (right) parentheses in $\pi$. Let $c(\pi)$ be the number of occurrences of the sequence () in $\pi$. Show that, among all the $\frac{1}{n+1}\binom{2n}{n}$ WFPs $\pi$ of size $n$, the average value of $c(\pi)$ is

$$\overline{c}(n) = ???.$$

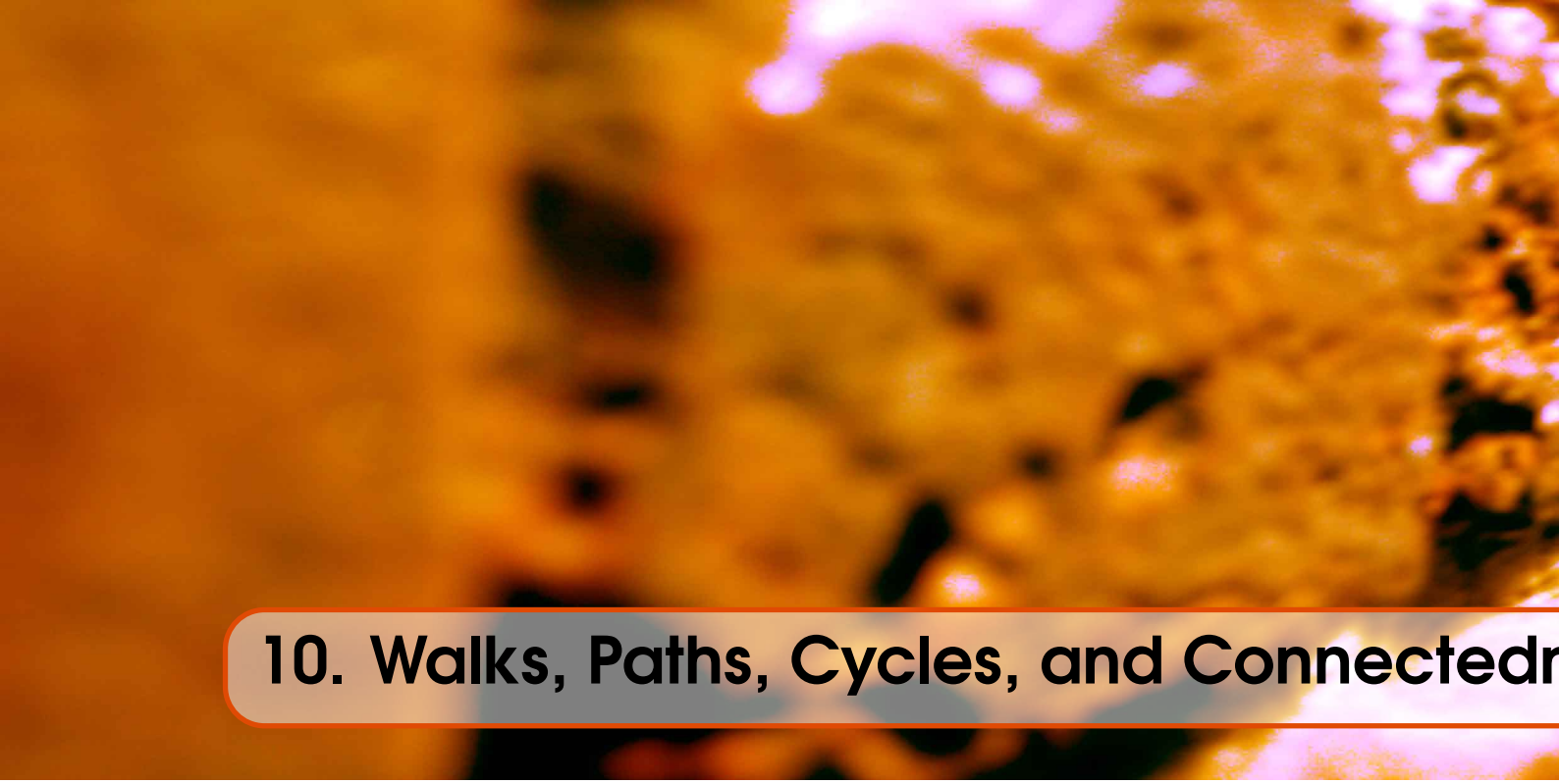
■

# Introduction to Graph Theory.



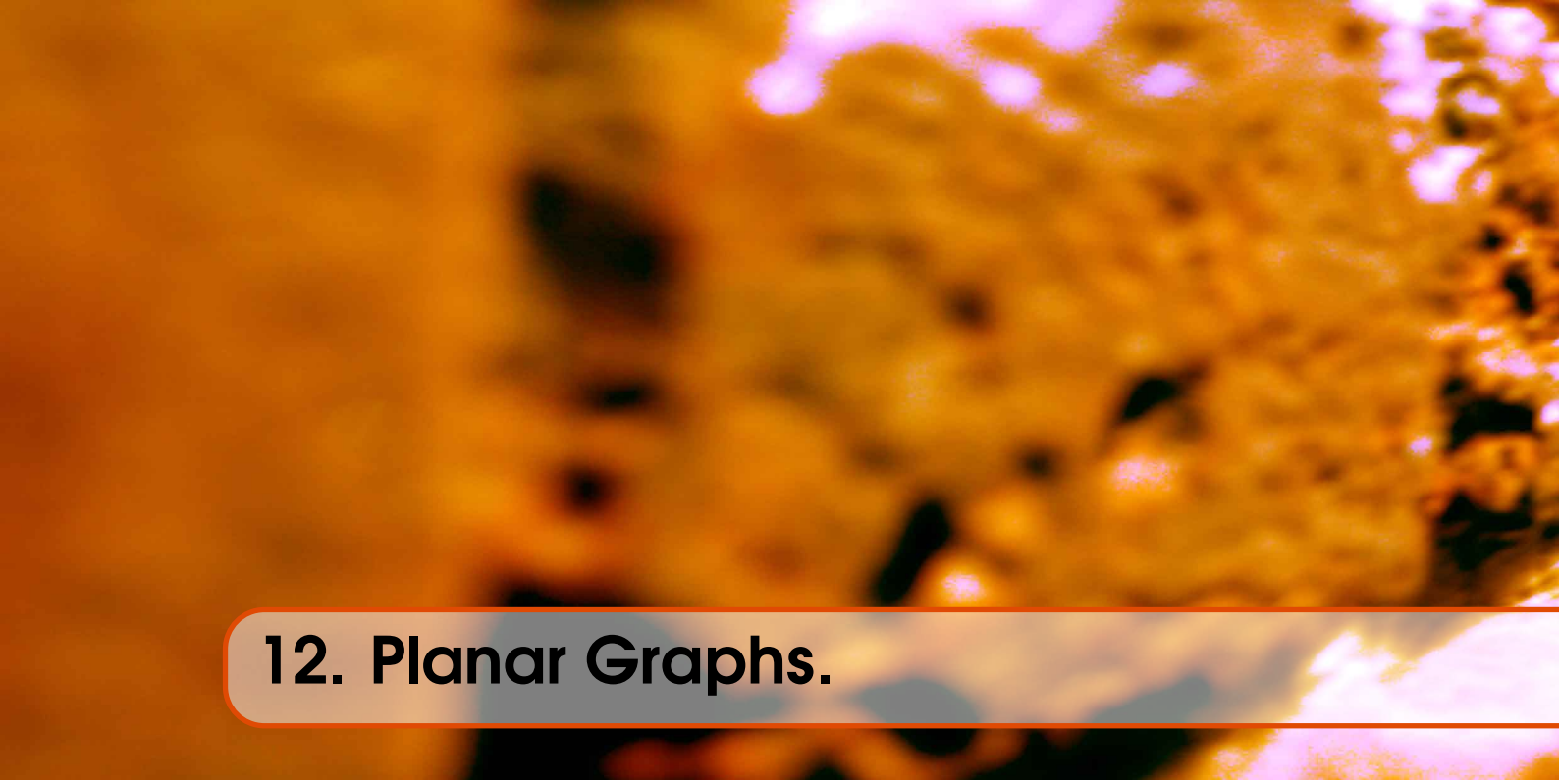
# 8. Introduction to Graph Theory.

# 9. Graphs and Isomorphism.

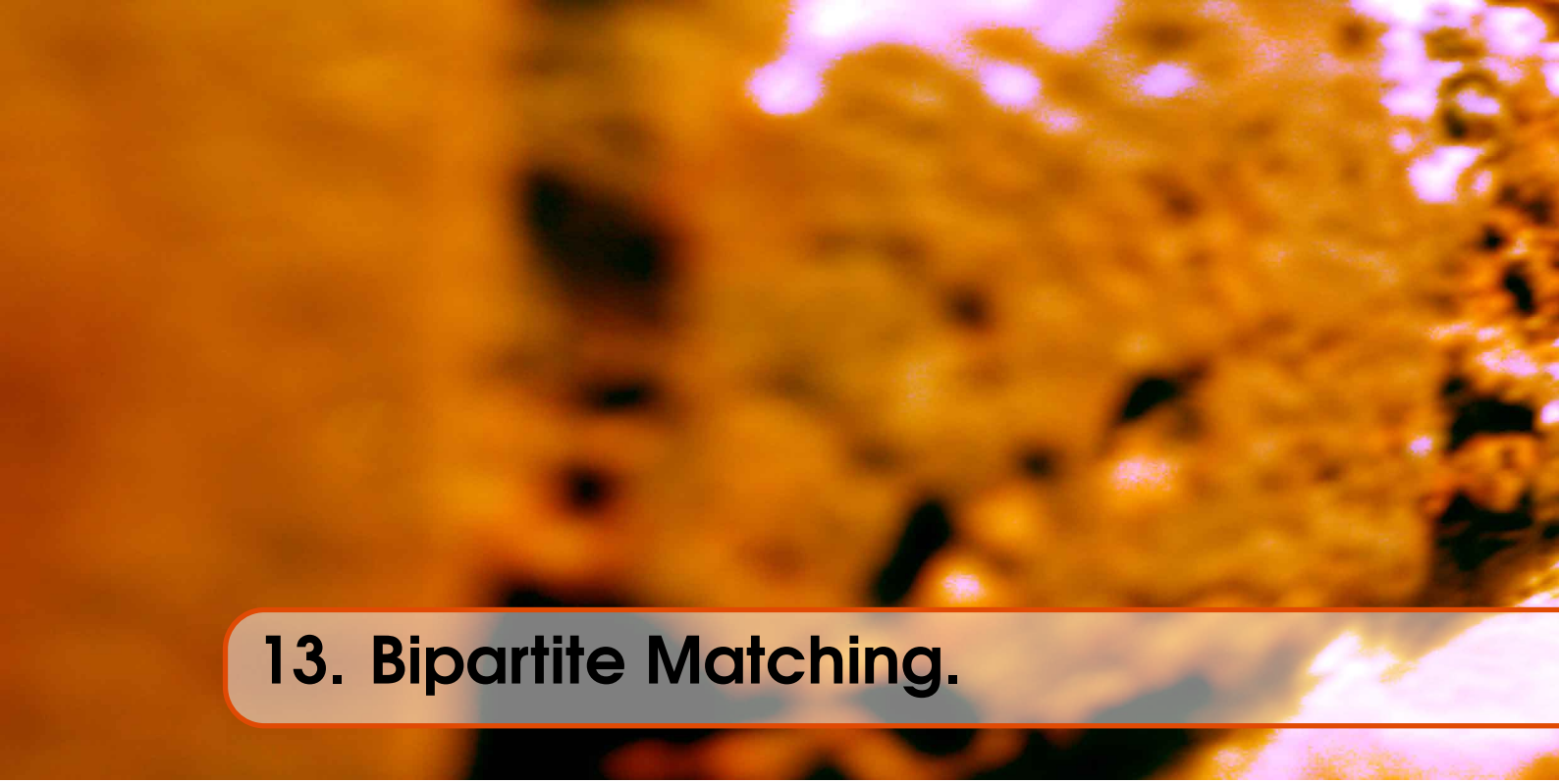


# 10. Walks, Paths, Cycles, and Connectedr

# 11. Trees.



# 12. Planar Graphs.



# 13. Bipartite Matching.

# Bibliography