2 An introduction to counting

One of the most important ways of summarizing a collection of objects is to count the number of elements in the collection. This doesn't sound difficult, but even if the collection is very easy to describe it may be very difficult to count. Here are some of the collections we will look at in this book, and the kinds of numbers which arise when we count them.

- The subsets of a fixed size in a given set.   [Binomial Coefficients]

- The onto functions between two finite sets.   [Stirling Numbers]

- The total collection of partitions of a set.   [Bell Numbers]

- The bracketings of a product of numbers.   [Catalan Numbers]

- The set of progeny of an ancestral pair of rabbits.   [Fibonacci Numbers]

We will see that complicated collections can often be expressed in terms of simple collections like the above, combined using simple rules. For example:

(1) **The Sum Rule.** If A and B are disjoint finite sets then the number of objects in $A \cup B$ is just the sum of the number of objects in A and the number of objects in B.

(2) **The Product Rule.** If A and B are disjoint finite sets then the number of objects in the cartesian product $A \times B$ (the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$) is just the product of the number of objects in A and the number of objects in B.

(3) **The One-to-One Correspondence Rule.** If the objects in A and the objects in B can be paired with one another in such a way that no objects of A or B are left over, then A and B have the same number of elemennts. [This is a useful way to count a collection of objects, which is analogous to the notion of congruence for comparing areas of regions. We can count a set of objects by finding another set (easier to count) which can be put in one-to-one correspondence with the first set.]

The most important of the numbers which arise in counting are the binomial coefficients. This is because, in counting a collection, we often count subsets, subsets of a given size and combinations of subsets. Thus in the first section we will introduce the binomial coefficients and at the same time gain some familiarity with partitions and Stirling numbers.

2.1 Counting functions

Let N and M be two sets with n and m elements respectively.

Problem. How may mappings $f \colon N \to M$ are there?

To answer this we need some notation.

Notation. Let m be a positive integer and N a set with n elements. We write

$$[n] = \{1, 2, \ldots, n\} \quad \text{(The set containing the first } n \text{ posititive integers.)}$$
$$|N| = (\text{the number of elements in } N) = n.$$

There are many ways to display a function. For purposes of counting, two descriptions are particularly convenient: as a matrix or as a string. In the first we display N as the top row of a matrix and write $f(x)$ under each element $x \in N$. Thus if $N = \{1, b, c, \ldots, d\}$, we write

$$f = \begin{pmatrix} a & b & c & \cdots & d \\ f(a) & f(b) & f(c) & \cdots & f(d) \end{pmatrix} \tag{1}$$

The elements $a, b, c, \ldots, d$ could stand for anythiing, for example for $1, 2, 3, \ldots, n$, if $n = |N|$. Hence if $n = |N|$, there are exactly as many functions $f \colon N \to M$ as there are functions

$$f \colon [n] \to M. \tag{2}$$

For functions of the form (2), it's natrual to display the elements of $[n]$ in order; so functions would look like:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix} \tag{3}$$

We can shorten (3) by eliminating the top row and wrtiing f as a string,

$$f(1)f(2)f(3)\cdots f(n), \tag{4}$$

or as

$$m_1 m_2 m_3 \cdots m_n, \tag{5}$$

where $f(i) = m_i$.

So, by the product rule, the total number of functions $f \colon [n] \to M$ is the same as the number of strings, namely

$$\underbrace{m \cdot m \cdot m \cdots m}_{n} = m^n.$$

Summarizing, we have

Counting all functions between two finite sets
Let N and M be two finite sets with n and m elements respectively.
The total number of functions $f \colon N \to M$ is given by

$$|M|^{|N|} = m^n.$$

(6)

Recall that a function $f \colon N \to M$ is *one-to-one* (or injective, or 1-1) if different elements have different images. In other words, if $f(x) = f(y)$ implies that $x = y$. One-to-one functions $f \colon N \to M$ correspond to strings of length n which contain no element of M twice. Hence we have:

Counting one-to-one functions between two finite sets
Let N and M be two finite sets with n and m elements respectively.
The total number of one-to-one functions $f \colon N \to M$ is

$$m(m-1)(m-2)\cdots(m-n+1) = m_{(n)}.$$

The number $m_{(n)}$ is often called the *falling factorial* of m.

(7)

For example, if $|N| = |M| = n$, then there are $n!$ one-to-one functions

$$f \colon N \to M.$$

Note. The image $f(N)$ of a one-to-one function $f \colon N \to M$ between finite sets N and M has the same size (or *cardinality*) as N.

The first difficulty arises when we count *onto* functions. Recall that a function $f \colon N \to M$ is *onto* (or surjective) if for any $x \in M$ there is a $y \in N$ for which

$$f(y) = x.$$

For exxample, if $|N| = |M|$ then every one-to-one function $f \colon N \to M$ is also onto. The function $f \colon N \to M$ is called a *bijection* if it is both one-to-one and onto.

Note. Bijections are just the *one-to-one correspondences* mentioned earlier.

Before attempting to count the onto functions between two sets, let us apply the above ideas to the problem of counting the number of subsets of a set.

Binomial coefficients

Problem. How many distinct subsets of size k are there in a finite set N?

First some notation. If $|N| = n$ and K is a subset of N with $|K| = k$ we say that N is an *n-set* and that K is a *k-subset* of N.

The number of k-subsets of an n-set is denoted by the *binomial coefficient* $\binom{n}{k}$.

The above problem is just the same as calculaating $\binom{n}{k}$. We argue as follows.

First, let K be a k-subset of N. There are $k!$ bijections $[k] \to K$. Hence there are $k!$ one-to-one functions $[k] \to N$ whose image is K. That is

$$(\text{\# of 1-1 functions } f \colon [k] \to N) = k! \cdot (\text{\# of } k\text{-subsets of } N). \tag{8}$$

By equation (7), the total number of one-to-one functions $[k] \to N$ is the $n_{(k)}$, so we must have

$$(\text{\# of 1-1 functions } f \colon [k] \to N = n_{(k)} = k! \binom{n}{k}. \tag{9}$$

Equation (9) now yields,

$$\boxed{\begin{array}{c} \textbf{Counting the number of subsets of a set} \\ \text{Let } N \text{ be a finite set with } n \text{ elements.} \\ \text{The total number of } k\text{-subsets of } N \text{ is given by} \\[2mm] \binom{n}{k} = \frac{n_{(k)}}{k!} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}. \end{array}} \tag{10}$$

Note. This is a very indirect way of finding $\binom{n}{k}$ and in the problems you will have a chance to learn more direct methods.

Partitions and Onto functions

Let us now look at onto function $f\colon N \to M$. The first thing to observe is that there are none if $|M| > |N$, (there are not enough elements of N to 'cover' the element of M). The second observation is that each onto function $f\colon N \to M$ determines a partition of N into $|M|$ parts.
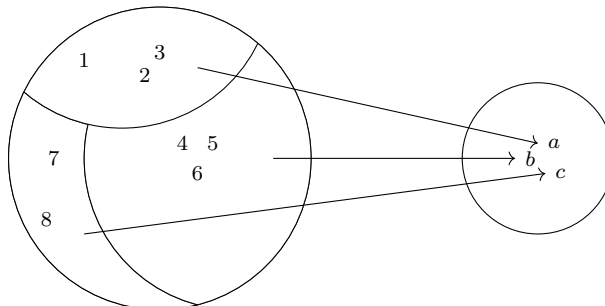

Figure 1. An onto function.

Definition. A *partition* of a finite set N into k parts (or blocks) is a family of subsets $N_1, N_2, \ldots, N_k$, of N with the properties:

(1) The union of all the N_i is the whole set N, i.e. $N_1 \cup N_2 \cup \cdots N_k = N$.

(2) the subsets are pairwise disjoint, i.e. $N_i \cap N_j = \emptyset$ for $i \neq j$.

Example 1. The partitions of the set $\{a, b, c, d\}$ into 3 parts can be displayed as the collection:

$$\{\{a\}, \{b\}, \{c\}, \{d\}\} \quad \{\{a\}, \{b, d\}, \{c\}\} \quad \{\{b\}, \{a, d\}, \{c\}\}$$
$$\{\{a\}, \{b, c\}, \{d\}\} \quad \{\{b\}, \{a, c\}, \{d\}\} \quad \{\{c\}, \{a, b\}, \{d\}\}$$

Or more simply

$$a|b|cd \quad a|bd|c \quad b|ad|c$$
$$a|bc|d \quad b|ac|d \quad c|ab|d$$

Notation. We write $S(n, k)$ for the number of partitions of an n-set into k parts. $S(n, k)$ is called a *Stirling number of the second kind*. From Example 1, we have $S(4, 3) = 6$.

Example 2. Let $N = \{a, b, c, d\}$ and consider the onto functions $f\colon N \to [3]$. We see that each onto function is completely determined by,

- a partition of N into 3 parts,

- a one-to-one function from the *partition* (as a set) to the set $[3]$.

For example: the partition $b|ac|d$ and the one-to-one function

$$\begin{pmatrix} \{b\} & \{a, c\} & \{d\} \\ 1 & 3 & 2 \end{pmatrix}$$

determine the onto function

$$\begin{pmatrix} a & b & c & d \\ 3 & 1 & 3 & 2 \end{pmatrix}$$

Conversely the onto function

$$\begin{pmatrix} a & b & c & d \\ 1 & 3 & 2 & 2 \end{pmatrix}$$

is completely determined by the partition $a|b|cd$ and the one-to-one function $f\colon \{\{a\}, \{b\}, \{c,d\}\} \to [3]$ defined by

$$\begin{pmatrix} \{a\} & \{b\} & \{c,d\} \\ 1 & 3 & 2 \end{pmatrix}.$$

The total number of onto functions $f\colon N \to [3]$ is thus (writing K for an arbitrary 3-set),

$$(\text{\# of 1-1 functions } f\colon K \to [3]) \cdot (\text{\# of partitions of } N \text{ into 3 parts})$$
$$= 2! S(4,3) = 3! \cdot 6 = 36.$$

The general case is just the same. If $|N| = n$, the number of N onto functions $f\colon N \to [k]$ is equal to

$$(\text{\# of 1-1 functions } f\colon K to [k]) \cdot (\text{\#partitions of } N \text{ into } k \text{ parts})$$
$$= k! S(n,k),$$

or

$$(\text{\# of onto functions } f\colon N \to [k]) = k! S(n,k). \tag{11}$$

Counting onto functions between two finite sets

Let N and K be two finites sets with n and k elements respectively.
The total number of onto functions $f\colon N \to K$ is
$$k! S(n,k).$$

The number $S(n,k)$ is called a *Stirling number of the second kind.*

(12)

Note. We see in (9) and (11) that the relationship between onto functions $f\colon N \to [k]$ and partitions of an n-set into k parts is similar to the relationship between one-to-one functions $f\colon [k] \to N$ and k-subsets of an n-set.

Conventions. So far we have avoided the inconvenient possiblity that M, or N, or both may be the empty set $\emptyset$. The following have proved with experience to be very useful conventions, and we will adopt them in this book.

- We will allow one function $\mathbf{1}_\emptyset \colon \emptyset \to \emptyset$, called the *identity function*. We will count this functio as one-to-one, so $0_{(0)} = 0! = 1$, $0^0 = 1$.

- We allow one function $\emptyset \to M$, for any set M. This function will also be treated as one-to-one, so $m_{(0)} = 1$, for $m > 0$. If N is non-empty then there are, of course, no function $N \to \emptyset$, and so no one-to-one functions, hence $0_{(n)} = 0$.

- There are no partitions of an non-empty set into zero parts, so $S(n,0) = 0$ for $n > 0$. But we will allow one partition of the empty set into zero parts, i.e. we define $S(0,0) = 1$.

Example 3. Suppose $|N| = n$, $|M| = m$. Let us count the collection of functions $f\colon N \to M$ in two ways. First, as strings, as in (6), to give m^n. Secondly, classify the functions depending on the size of their images. The number of functions with image $f(N) = K \subseteq M$ is just the number of onto

functions $f\colon N \to K$, which from (12) is $k!S(n,k)$ if $|K| = k$. Hence the total number of functions $f\colon N \to M$ with image of size k is

$$(\# \text{ of } k\text{-subsets } K \text{ of } M) \cdot (\# \text{ of onto functions } f\colon N \to K)$$

$$= \binom{m}{k} k! S(n,k),$$

where we have used (10) and (12).

Since the image of f may have $0, 1, 2, \ldots$, of n elements, we obtain the following important combinatorial identity:

$$m^n = \sum_{k=0}^{n} \binom{m}{k} k! S(n,k)$$

$$= \sum_{k=0}^{n} S(n,k) m_{(k)} \tag{13}$$

Using the conventions above, identity (13) encompasses all possible choices for n and m.

Note. In classifying the objects of a collection for counting purposes, as above, it's important to remember that each object to be counted must occur in one and only one class (so that the conditions of the sum rule are satisfied).

Example 4. Identity ((13)) may be used directly to evaluate the numbers $S(n,m)$ by solving systems of equations. For $n = 4$, ((13)) gives the system

$$0^4 = 0,$$
$$1^4 = S(4,1)1_{(1)},$$
$$2^4 = S(4,1)2_{(1)} + S(4,2)2_{(2)},$$
$$3^4 = S(4,1)3_{(1)} + S(4,2)3_{(2)} + S(4,3)3_{(3)},$$
$$4^4 = S(4,1)4_{(1)} + S(4,2)4_{(2)} + S(4,3)4_{(3)} + S(4,4)4_{(4)}.$$

This yields a system of four equations in four unknowns whose coefficient matrix has non-zero determinant, and so the system has a unique solution for the numbers $S(4,1)$, $S(4,2)$, $S(4,3)$, $S(4,4)$. Solving we find

$$S(4,1) = 1, \quad S(4,2) = 7, \quad S(4,3) = 4, \quad S(4,4) = 1.$$

Remark. In later sections, we will see how to easily solve such systems of equations. We will also find simple computational formulas for the Stirling numbers, using other techniques.

2.1.1 Exercises

1. Find the numbers $S(5,k)$ for $k = 0,1,2,3,4,5$, directly by counting partitions, and secondly, by using the identity (15).

2. Count the number of functions from an n-set to an $m+1$-set in two ways to obtain the identity.

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

See Example 4, Chapter 2

2.2　The binomial theorem and multinomial coefficients

Let N, M be sets, A and B subsets of M such that $M = A \cup B$ and $A \cap B = \emptyset$ (A or B may be empty), and $|N| = n$, $|A| = a$, $|B| = b$ and $|M| = a + b = m$. By (6) there are $(a+b)^n$ functions $f \colon N \to M$. We can count the functions also in of N whose image lies in A. For example, let Class 0 contain those functions mapping 0 elements of N to A. There are, by (6), b^n such functions. Let Class 1 contain those functions which map one element of N to A. The element to be mapped to A can be selected in $\binom{n}{1}$ ways and there are a possible images for it. The remaining elements can be mapped to B in b^{n-1} ways. Hence Class 1 contains $\binom{n}{1}ab^{n-1}$ elements. Proceeding in this way we find that Class k (all functions mapping k elements of N to A) contains $\binom{n}{k}a^k b^{n-k}$ elements. Since functions $f \colon N \to M$ may have $0, 1, 2, \ldots$, or n elements mapping to A, we obtain the *binomial identity*,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{14}$$

In particular, if $a = b = 1$ we obtain,

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n. \tag{15}$$

Note.. The word 'binomial' refers to expressions with two terms. The name '*binomial coefficient*' is due to the occurrence of these numbers in identity (14).

The argument which leads to (14) easily generalizes to more than two sets. Thus we have the *trinomial identity*

$$(a + b + c)^n = \sum_{\substack{i,j,k \\ i+j+k=n}} \binom{n}{i, j, k} a^i b^j c^k, \tag{16}$$

where summation is over all triples (i, j, k) of non-negative integers with $n = i + j + k$, and where the coefficients are given by

$$\binom{n}{i, j, k} = \binom{n}{i}\binom{n-i}{j} = \frac{n!}{i!j!(n-i-j)!}. \tag{17}$$

In general, we have the *multinomial identity*,

$$(a_1 + a_2 + \cdots + a_p)^n = \sum_{\substack{i_1, i_2, \ldots, i_p \\ i_1 + i_2 + \cdots + i_p = n}} \binom{n}{i_1, i_2, \ldots, i_p} a_1^{i_1} a_2^{i_2} \cdots a_p^{i_p}.$$

The coefficients in (18) are called *multinomial coefficients* and, by the same argument as for binomial coefficients, are given by,

$$\begin{aligned}
\binom{n}{i_1, i_2, \ldots, i_p} &= \binom{i_1 + i_2 + \cdots + i_p}{i_1, i_2, \ldots, i_p} \\
&= \binom{n}{i_1}\binom{n-i_1}{i_2}\binom{n - i_1 - \cdots - i_{p-1}}{i_p} \\
&= \frac{n!}{i_1! i_2! \cdots i_p!}
\end{aligned} \tag{19}$$

2.2.1 Exercises with Answers

1. Consider the product $(a^2 + b^3 + c^4)^{10}$. Find the coefficients of $a^4b^6c^{24}$, $a^6b^{12}c^{12}$ and $a^{12}b^9c^{24}$. [Answer:1260; 4200;0]

2. A *division* of a set N into k parts is a p-tuple of subsets $(A_1, A_2, \ldots, A_p)$, some of which may be empty, satisfying the conditions,

(i)) $N = A_1 \cup A_2 \cup \cdots \cup A_p$;

(ii) $A_i \cap A_j = \emptyset$, for $i \neq j$.

Show that the number of divisions $(A_1, A_2, \ldots, A_p)$ of N with $|N| = n$, $|A_k| = i_k$, for $i = 1, \ldots, p$ is the multinomial coefficient $\binom{n}{i_1, i_2, \ldots, i_p}$.

2.3 Binomial coefficients

In counting problems it is often useful to consider sub-collections of the collection of objects to be counted. There is an analogy here with integration. We can find the mass of a length of wire by looking at the mass of small pieces of the wire. Similarly in Example 3 we were able to count the set of functions $f \colon N \to M$ in two ways to give the identity

$$m^n = \sum_{k=0}^{n} S(n,k)m_{(k)} \tag{20}$$

Here we have some 'global information' (that there are m^n functions $f \colon N \to M$) and some 'local information' about the set of functions with image of a given size. Equation (20) relates these two types of information. As a biproduct we obtain a very useful information concerning the Stirling numbers. In this section we study the binomial coefficients by looking at sub-collections in different ways.

Example 5. (Symmetry of Binomial Coefficients.) Formula (10) for the value of the binomial coefficient $\binom{n}{k}$ is clearly symmetric with respect to k and $n - k$. The identity

$$\binom{n}{k} = \binom{n}{n-k}, \tag{21}$$

expresses the fact that there is a one-to-one correspondence (pairing) between subsets of an n-set and $n - k$-subsets of an n-set given by the mapping $A \mapsto \bar{A}$, where $\bar{A}$ is the complement of the subset A in the n-set.

Example 6. (Product properties of Binomial Coefficients.) Suppose again N is an n-set. Let's count all sets of the form $\{x, A\}$ where A is a k-subset of N and $x \in A$. We can do this in two ways. Since there are $\binom{n}{k}$ ways of choosing A and then k choices for x, the total number of sets $\{x, A\}$ must be $k\binom{n}{k}$.

Alternatively, we can choose x first (in n ways) and then 'build A around x' by choosing a further $k - 1$ elements from the set $N - \{x\}$. There are $\binom{n-1}{k-1}$ ways of doing this so the total number of sets $\{x, A\}$ is also $n\binom{n-1}{k-1}$.

Of course it is implicit in our discussion that $k \neq 0$, hence we have the simple product rule

$$k\binom{n}{k} = n\binom{n-1}{k-1}, \qquad \text{for } k \neq 0. \tag{22}$$

You would have discovered this rule easily by manipulating formula (10). However we can generalize our counting problem to give a less obvious product rule. Let us count the collection of sets of the form $\{B, A\}$, where A is a k-subset of N and B is a l-subset of A. The first way of counting clearly yields $\binom{n}{k}\binom{k}{l}$.

In the second case we choose subset B first in $\binom{n}{l}$ ways, then "build" A around B from the remaining $n - l$ elements of $N - B$, in $\binom{n-l}{k-l}$ ways. Hence we have an important identity,

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}, \qquad \text{for } l \leq k. \tag{23}$$

Example 7. (**Vandermonde's identity**) Is there some way to express the binomial coefficient $\binom{m+w}{k}$ in terms of binomial coefficients of m and w?

The answer is yes, and we see why if we think of choosing k people from a group of m-men and n-women. Now we can use the classification technique. In choosing k people we can choose either $0, 1, \ldots,$ or k men and the rest women. We can choose k people l of whom are men in $\binom{m}{l}\binom{w}{k-l}$ ways. Putting all this together, we have the identity named after the Dutch mathematician, Abnit-Theophile Vandermonde (1735-1796).

$$\binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{w}{k-1} + \cdots + \binom{m}{k}\binom{w}{0} = \binom{m+w}{k}. \tag{24}$$

Example 8. (**Pascal's identity**) The special case of (24) with $m = 1$ yields the identity,

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}. \tag{25}$$

[In other words, we can choose k-people from m men and one woman by choosing just men, or the woman together with $k - 1$ men.]

Identity (25) is course the basis of Pascal's Triangle of binomial coefficients.

$$
\begin{array}{ccccccc}
& & & \binom{0}{0} & & & \\
& & \binom{1}{0} & & \binom{1}{1} & & \\
& \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\
& \vdots & & \vdots & & \vdots &
\end{array}
\qquad
\begin{array}{ccccccc}
& & & 1 & & & \\
& & 1 & & 1 & & \\
& 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1 \\
& \vdots & & \vdots & & \vdots &
\end{array}
$$

The First Four Rows of Pascal's Triangle

The identities given in the above examples combine to yield countless further identities.

Example 9. (**Summation formulas**) Repeated application of Pascal's identity yields

$$
\begin{aligned}
\binom{m+1}{k} &= \binom{m}{k} + \binom{m}{k-1} \\
&= \binom{m}{k} + \binom{m-1}{k-1} + \binom{m-1}{k-2} \\
&\vdots \\
&= \binom{m}{k} + \binom{m-1}{k-1} + \cdots + \binom{m-k}{0}.
\end{aligned}
$$

15

Or better, replacing m by $n + k$ we have

$$\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}. \tag{26}$$

Alternatively, we can rewrite (25) as:

$$\begin{aligned}
\binom{m+1}{k+1} &= \binom{m}{k} + \binom{m}{k+1} \\
&= \binom{m}{k} + \binom{m-1}{k} + \binom{m-1}{k+1} \\
&\vdots \\
&= \binom{m}{k} + \binom{m-1}{k} + \cdots + \binom{m-(m-k)}{k} + \binom{m-(m-k)}{k+1}.
\end{aligned}$$

The last term is zero, so we have the identity

$$\binom{k}{k} + \binom{k+1}{k} + \cdots \binom{m}{k} = \binom{m+1}{k+1}. \tag{27}$$

Identites arising from the Binomial Theorem

From the binomial identity (14), taking $b = 1$, we have

$$(1+a)^n = \sum_{k=0}^{n} \binom{n}{k} a^k, \tag{28}$$

which is satisfied by all positive integer values of a. This means that the polynomial

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

has infinitely many distinct roots, and so by the fundamental Theorem of Algebra, is the unique polynomial having that property, namely the zero polynomial. Hence we obtain from (28), the polynomial identity,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{29}$$

We can now perform operations on (29), like multiplication, differentiation and integration, and obtain identites by comparing coefficients, or substituting values for x.

Example 10. The product

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

yields

$$\left[\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n \right] \left[\binom{m}{0} + \binom{m}{1}x + \cdots + \binom{m}{m}x^m \right]$$

$$= \binom{n+m}{0} + \binom{n+m}{1}x + \cdots + \binom{n+m}{n+m}x^{m+n} \tag{30}$$

16

Comparing coefficients of x^k on both sides of (30) now yields

$$\sum_{i=1}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \cdots + \binom{n}{k}\binom{m}{0} = \binom{n+m}{k} \tag{31}$$

The special case with $k = n$ of $k = m$ is just Vandermonde's identity.

Example 11. Differentiate (29) to obtain

$$n(1+x)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1}. \tag{32}$$

Substituting $r = 1$ gives

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + (n-1)\binom{n}{n-1} = n2^{n-1}.$$

Remark.. The Fundamental Theorem of Algebra generalizes to the following. Let $N_1, N_2, \ldots, N_p$ be infinite sets of rational numbers and $f(x_1, x_2, \ldots, x_p)$ and $g(x_1, \ldots, x_p)$ polynomials satisfying

$$f(a_1, a_2, \ldots, a_p) = g(a_1, a_2, \ldots, a_p),$$

for all $a_i \in N_i$, $1 \le i \le p$. Then f and g are identically equal. Using this result, the combinatorial identity (18), becomes the multinomial identity between polynomials,

$$(x_1 + x_2 + \cdots + x_p)^n = \sum_{\substack{i_1, i_2, \ldots, i_p \\ i_1+i_2+\cdots+i_p=n}} \binom{n}{i_1, i_2, \ldots, i_p} x_1^{i_1} x_2^{i_2} \cdots x_p^{i_p} \tag{33}$$

Combining Simple Identites

We have seen how to obtain a number of identities involving binomial coefficients by counting collections of objects in different ways. These identties can be manipulated and combined to give an endless variety of binomial identities (usually not associated with any obvious counting problem). The binomial identites have a certain aesthetic appeal, apart from their common appearance in many parts of mathematics and their usefulness in such areas of computer science as the analysis of algorithms.

Example 12. Simplify $\displaystyle\sum_{k=l}^{n} \binom{n}{k}\binom{k}{l}$.

Applying identity (23) we get

$$\sum_{k=l}^{n} \binom{n}{k}\binom{k}{l} = \sum_{k=l}^{n} \binom{n}{l}\binom{n-l}{k-l}$$

$$= \binom{n}{l} \sum_{k=l}^{n} \binom{n-l}{k-l}.$$

Now (14) gives the result

$$\sum_{k=l}^{n} \binom{n}{k}\binom{k}{l} = \binom{n}{l} 2^n. \tag{34}$$

The proof is by induction on p. For details see for example the book by Serge Lang, "*Algebra*" Addison-Wesley (1965) p. 122.

See for example, the 1972 standardized table of 500 binomial identities, compiled by H.W. Gould, West Virginia University, Morgantown, W. Va.

See Donald E. Knuth's, "*The Art of Computer Programming Volume 1: Fundamental Algorithms*" Addison-Wesley (1969) for a thorough account of the interrelationship between combinatorics and computer science.

2.3.1 Exercises

1. Show in two ways (first using formula (10), and second, finding an appropriate counting problem) that:

(i) $(n-k)\binom{n}{k} = n\binom{n-1}{k}$ for $k \le n$ and $n \ne 0$.

(ii) $\binom{n}{k}\binom{n-k}{l} = \binom{n}{l}\binom{n-l}{k}$, for $l \le n-k$ and $k \le n$.

2. Sum the following:

(i) $\binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \binom{m}{2}\binom{n}{2} + \cdots + \binom{m}{n}\binom{n}{n}$. [Answer: $\binom{m+n}{n}$]

(ii) $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2$. [Answer: $\binom{2n}{n}$]

3.

(i) Prove that $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i} = \begin{cases} 0, & \text{if } n \ne 0, \\ 1, & \text{if } n = 0. \end{cases}$

(ii) Determine from (i) and identity (23) that

$$\sum_{i=m}^{n}(-1)^{m+i}\binom{n}{i}\binom{i}{m} = \begin{cases} 0, & \text{if } m \ne n, \\ 1, & \text{if } m = n. \end{cases}$$

4. Prove the following identites for n, m, r positive integers.

(i) $\binom{n}{m}\binom{r}{0} + \binom{n-1}{m-1}\binom{r+1}{1} + \cdots + \binom{n-m}{0}\binom{r+m}{m} = \binom{n+r+1}{m}$

(ii) Show that $\binom{x+1}{m+1} = \binom{x}{m+1} + \binom{x}{m}$ is a polynomial identity. [Note that $\binom{x}{m} = \dfrac{x_{(m)}}{m!}$.]

2.4 Stirling numbers

As we have seen, a partition of a set is a family of disjoint subsets which 'cover' the set. Such families are important when we try to count a collection of objects. As we have seen Stirling numbers (of the *second* kind) arise when we count partitions, so these are probably the most common numbers occurring in counting problems, after binomial coefficients. They are harder to deal with than binomial coefficients (we have no simple formula like (10) for them) but we have a useful recurrence relation similar to Pascal's identity which is satisfactory for small values of n and k.

A Pascal-type triangle for Stirling numbers

Consider an arbitrary set with $n+1$ elements, say $\{x_1, x_2, \ldots, x_{n+1}\}$. Let us count the partitions of this set into k parts, or blocks. By definition, there are $S(n+1, k)$ such partitions. But we can count them in an alternate way, by counting those partitions that have $\{x_{n+1}\}$ as a block and those that don't.

If $\{x_{n+1}\}$ is a block of the partition we need to divide the set $\{x_1,\ldots,x_n\}$ into $k-1$ blocks and there are $S(n,k-1)$ ways of doing this.

If $\{x_{n+1}\}$ is not a block, then x_{n+1} must be contained in a block with at least one other element of the set. There are $S(n,k)$ ways of partitioning $\{x_1,x_2,\ldots,x_n\}$ into k blocks and x_{n+1} may lie in any one of these blocks. Hence there are a total of $kS(n,k)$ ways in which the original set can be partitions into k blocks without $\{x_{n+1}\}$ being a block.

Putting all this together we obtain the recurrence relation for the Stirling numbers of the second kind.

$$S(n+1,k) = S(n,k-1) + kS(n,k). \tag{35}$$

In addition we have the obvious initial conditions,

$$\begin{aligned} S(n,1) &= 1, \\ S(n,n) &= 1, \quad \text{for } n \geq 1, \end{aligned} \tag{36}$$

This yields the following triangle for the Stirling numbers of the second kind.

$$
\begin{array}{ccccccccc}
& & & & S(1,1) & & & & \\
& & & S(2,1) & & S(2,2) & & & \\
& & S(3,,1) & & S(3,2) & & S(3,3) & & \\
& S(4,,1) & & S(4,2) & & S(4,3) & & S(4,4) & \\
S(5,,1) & & S(5,2) & & S(5,3) & & S(5,4) & & S(5,5) \\
\vdots & & \vdots & & \vdots & & \vdots & &
\end{array}
$$

$$
\begin{array}{ccccccccc}
& & & & 1 & & & & \\
& & & 1 & & 1 & & & \\
& & 1 & & 3 & & 1 & & \\
& 1 & & 7 & & 6 & & 1 & \\
1 & & 15 & & 25 & & 10 & & 1 \\
& \vdots & & \vdots & & \vdots & & \vdots &
\end{array}
$$

The First Five Rows of Stirling Numbers

2.4.1 Exercises

1. Show that $S(n,k)m_{(k)}$ is the number of ways of placing n balls in m boxes so that exactly $m-k$ boxes remain empty.

2. Prove the recurrence relation

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

3. The nth *Bell number*, B_n is the number of partitions of a set with n elements. Establish the recurrence formula

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

2.5 Lattice paths

In this section we give a different interpretation of binomial coefficients, in terms of counting paths in the lattice of integer lines. This will yield quite different "combinatorial proofs" of many binomial identities.

Consider the lattice of integer lines on the cartesian plane as shown in the diagram. Let (m, n) be a fixed point on this lattice.

We define an *increasing path* from $(0,0)$ to (m, n) to be an ordered set of edges $(e_1, e_2, \ldots, e_k)$ from the lattice which have the following properties:

(i) e_i has a vertex in common with both e_{i-1} and e_{i+1} for $i = 2, 3, \ldots, k - 1$; i.e. the edges make a connected path from $(0,0)$ to (m, n).

(ii) In going from one vertex to another, the path either increases in x or increases in y.

The path shown in the diagram could be represented by the sequence:

$$x \; y \; y \; x \; x \; y \; x \; y \; x \; x \; y.$$

Problem.. How many increasing paths are there from $(0,0)$ to (m, n)?

To answer this, notice first that each path must increase in x exactly m times and in y exactly n times, so each sequence will have a total of $m + n$ x's and y's. The total number of sequences is thus the number of ways of assigning x's and the y's to the $m + n$ possible places in th sequence, i.e.

The Number of Increasing Lattice Paths.

The number of increasing lattice paths from the point $(0,0)$ to the point (m, n) is

$$\binom{n + m}{m} = \binom{n + m}{m}$$

(37)

Remark. We content ourselves with the lattice path proof of identity (26) and leave the interpretation of several other identities as problems.

Example 13. Consider the point $(m, n + 1)$. The total number of increasing paths from $(0,0)$ to $(m, n + 1)$ is, by (37) , $\binom{n+m+1}{m}$.

However, we can count the paths in another way. Consider the pints $(0, n+1), (1, n+1), \ldots, (m, n+1)$. As soon as a path reaches one of those points, its rout to $(m, n+1)$ is then completely determined. So

the paths can be classified according to which of the points $(0, n), (1, n), \ldots, (m, n)$ *precedes* the entry of the path to the line $y = n + 1$.
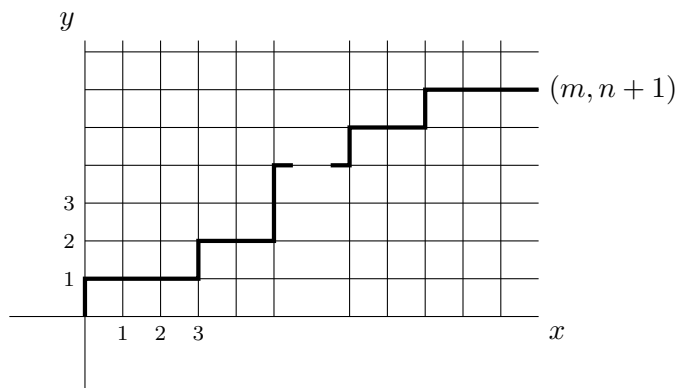
There are

- $\binom{n}{0}$ paths with enter at $(0, n)$,

- $\binom{n+1}{1}$ paths with enter at $(1, n)$,

- $\binom{n+2}{2}$ paths with enter at $(2, n)$,

and so on. Hence we obtain the identity,

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+m}{m} = \binom{n+m+1}{m}, \tag{38}$$

which is of course just the same as (26).

2.5.1 Exercises.

1. Give lattice path interpretations of the following identities:

(i) $\binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}$.

[Hint: Consider the increasing lattice paths from $(0, 0)$ to $(m - k, k + 1)$ for $m \geq k$.]

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

(iii) Vandermonde's identity.

2.6 Error correcting codes

We finish this introductory chapter by looking at one important application in which binomial coefficients occur: to finding bounds on the maximal number of codewords that can occur in an *error-correcting code*.

A *binary block code* is a set of "words" (*codewords*) made up of 0's and 1's and all having the same length, say n. The *distance* between codewords is defined to be the number of places in which the codewords differ.

For example, the distance between the codewords 0110101 and 1010111 is 3.

A codeword may become garbled in transmission. In this case how should the receiver interpret the incoming string? A good strategy would be for the receiver to find the codeword closest to the string received. If there is a *unique* codeword closest to the string received then it would be reasonable to assume that this was the intended codeword.

The aim of constructing codes is to keep the codewords far enough apart so that garbled words can be interpreted.

Suppose we have a binary block code with words of length n. Let the minimum distance between any two codewords be $2r + 1$, for a positive integer r. Then if we consider the circles of radius r about the codewords, these do not intersect and hence if a codeword is transmitted with at most r errors the transmitted string is nearest the correct codeword. We call such a code an *r-error correcting code*. On the other hand, spacing the words far apart will allow only a few codewords of a given length n.
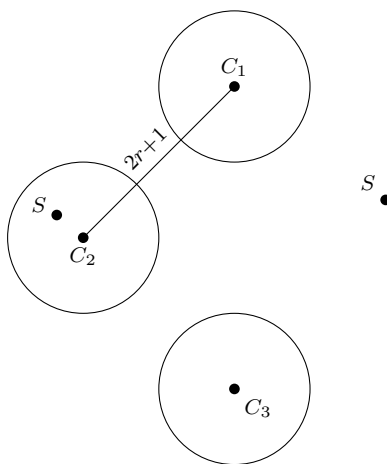
Let $M(n, r)$ denote the maximum number of codewords in an r-error correcting code.

For each codeword, there are many other strings which cannot be codewords. For example, none of the strings having distance $1, 2, \ldots,$ or r from the codeword can themselves be codewords. Let's count the number of strings that are excluded from the code by a given codeword.

- There are those which differ by 1 digit. Since each digit can be only 0 or 1, there are $n = \binom{n}{1}$ of these.

- There are those which differ by 2 digits. There are many of these as there are ways of choosing the 2 digits from a set of n, namely $\binom{n}{2}$ such strings.

- There are those which differ by 3 digits and so on. In general there are $\binom{n}{k}$ strings which differ from a given codeword by k digits.

We conclude that each codeword in an r-error correcting binary block code accounts for a total of (including the codeword itself)

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$$

strings of length n. In §1 we saw that there were 2^n binary strings of length n. Hence we must have

$$M(n,r)\left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}\right] \leq 2^n. \tag{39}$$

Alternatively, we can rewrite (39) as

$$M(n,r) \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}. \tag{40}$$

Inequality (40) is called the *Hamming bound* on the maximum number of codewords in an r-error correcting code.

Example 14. If $N = 6$ and $r = 1$, (40) tells us that the maximum number of codewords of length 6 which could correct one error is

$$M(6,1) \leq \frac{2^6}{1 + \binom{6}{1}} = \frac{64}{7} \approx 9.14.$$

In fact the best we can do is eight codewords, for example

$$\begin{array}{cccc} 000000 & 100110 & 001111 & 101001 \\ 010011 & 110101 & 011100 & 111010 \end{array}$$

2.6.1 Exercises

1. Suppose n different letters can be transmitted through a communication channel. How many different messages consisting of m letters are possible if

(i) letters can be used repeatedly in each messsage;

(ii) each letter can appear at most once in a message;

(iii) k of the letters can be used only for the beginning or end of the message (but not both), all other letters can be used, with possible repetition, inside the message.

2. Proteins are constructed from amino acids which are coded in the RNA molecule by triplets of the four bases A, U, G, C (adenine, uracil, guanine and cytosine). Determine the number of

(i) unordered triplets;

(ii) ordered triplets;

(iii) ordered triplets in which the middle base is significant but the end bases may occur in either order (e.g. $ACG = GCA$ but $ACG \neq AGC$).

3. Establish the *Gilbert lower bound*,

$$M(n,r) \geq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{2r}}. \tag{41}$$

2.7 Problems

1. In how many ways can the letters x, y, z, w, w, w, w be ordered so that no two w's are adjacent?

2. Show that the number of different ways in which m distinct numbers from $[n]$ can be arranged in a circle is

$$\frac{n!}{m(n-m)!},$$

if arrangements which differ by rotations are considered the same.

3. A bijection $N \to N$ is a called a *permutation* f the set N. Find the number of permutations of $[2n]$ in which even numbers are mapped to even numbers.

4. A partition of $[n]$ is said to be of type $(k_1, k_2, \ldots, k_n)$ if it has k_i blocks of size i. If $k_1, k_2, \ldots, k_n$ are non-negative integers, show that the total number of partitions of type $(k_1, k_2, \ldots, k_n)$ is

$$\frac{n!}{k_1!(1!)^{k_1} \cdot k_2(2!)^{k_2} \cdots k_n(n!)^{k_n}}.$$

5. Suppose that $a_1 \le a_2 \le \cdots \le a_k$ is a sequence of k elements from the set $[m]$ and conisder the associated subset $\{a_1, a_2 + 1, \ldots, a_k + (k-1)\}$ of $[m+k-1]$.

   (i) Show that this correspondence between sequences and subsets is one-to-one and onto.

   (ii) Deduce that the number of ways of choosing k things from m things (allowing repetitions) is $\binom{m+k-1}{k}$.

6. Given a set N of size n, show that the number of ways to choose k things from N, allowing repetition is the number of n-tuples of natural numbers $(x_1, x_2, \ldots, x_n)$ such that

$$x_1 + x_2 + \cdots + x_n = k.$$

7. Consider a set of $2n$ objects, n of which are identical. How many ways are there of choosing n objects from the set?

8. A flag is divided into n vertical stripes which are to be colored so that adjacent stripes have different colors. In how many ways can this be done?

9. In how many ways can three distinct integers be selected from $[600]$ so that their sum is divisible by 3?

10. Consider a polygon with n sides (an n-gon), in which no three diagonals (lines joining non-adjacent vertices) intersect at a common point. If all possible diagonals are drawn in such an n-gon, how many intersection points will there be?

11. Show that the number of ways of arranging m one's and n zero's in a row such that no two one's are adjacent is $\binom{n+1}{m}$.

12. Show that $\binom{n}{k-1} < \binom{n}{k}$ for $1 \le k \le n/2$ and that $\binom{n}{k} < \binom{n+1}{k}$ for $1 \le k \le n$.

13. Show that the number of subsets of $[n]$ consisting of k elements, no two of which are consecutive integers, is

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

14. Find closed forms for $\sum_{j=0}^{n} j^k \binom{n}{j}$ for $k = 2$ and $k = 3$.

15. Define the polynomial $x^{(n)}$ (the nth rising factorial of x) by

$$x^{(n)} = x(x+1)(x+2)\cdots(x+n-1).$$

Establish the polynomial identity
$$\frac{(x+1)^{(n)}}{n!} = \sum_{k=0}^{n} \frac{x^{(k)}}{k!}.$$

(i) Show that $m^{(n)}$ is the number of ways of arranging n objects in m stacks, where the order withini each stack is important and it is allowable for some stacks to be empty.

(ii) Show that the number of ways of arranging n objects in m non-empty stacks is

$$n!\binom{n-1}{m-1}.$$

(iii) Deduce from (i) and (ii) that

(a) $x^{(n)} = \displaystyle\sum_{k=1}^{n} \frac{n!}{k!}\binom{n-1}{k-1} x_{(k)}.$

(b) $x_{(n)} = \displaystyle\sum_{k=1}^{n} (-1)^{n+k} \frac{n!}{k!}\binom{n-1}{k-1} x^{(k)}.$

The integers $(-1)^n \dfrac{n!}{k!}\dbinom{n-1}{k-1}$ are called *Lah numbers*.

16. Show that
$$k!S(n,k) = \sum \binom{n}{i_1, i_2, \ldots, i_k},$$
where the sum is over all the k-tuples of positive integers $(i_1, i_2, \ldots, i_k)$ such that $i_1 + \cdots + i_k = n$.

17. The *Stirling numbers of the first kind* $s(n,m)$ are defined as the connection coefficients in the polynomial identities,
$$x_{(n)} = \sum_{k=0}^{n} s(n,k)x^k,$$
where $x_{(n)} = x(x-1)(x-2)\cdots(x-n+1)$. Establish the following formulas for the Stirling numbers of the first kind:

(i) $s(n,1) = (-1)^{n-1}(n-1)!.$

(ii) $s(n,n-1) = \binom{n}{2}.$

(iii) $s(n+1,2) = (-1)^{n+1}(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n})n!.$