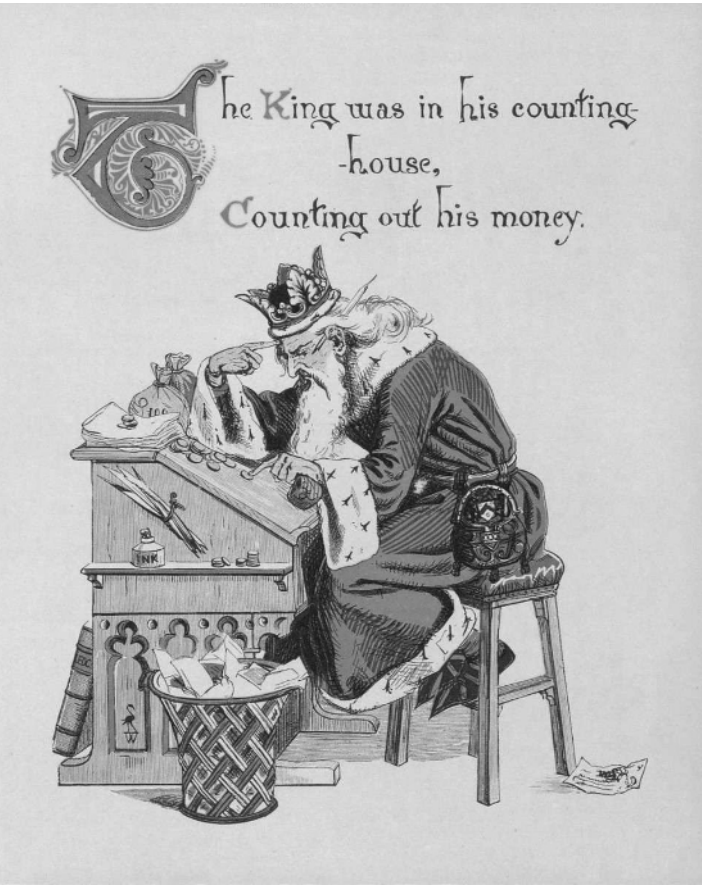
PART I

MATHEMATICAL PRELIMINARIES

CHAPTER 1

Counting



Walter Crane (1814–1915), *The Song of Sixpence*: "The Queen was in the parlor, eating bread and honey."

This chapter reviews the basic counting techniques that will be used throughout the book. An excellent reference for this material is [Rosen 2003].

1.1 THE SUM AND PRODUCT RULES

SUM RULE

If the first of two tasks can be performed in any of n_1 ways and the second in any of n_2 ways, and if these tasks cannot be performed at the same time, then there are $n_1 + n_2$ ways of performing either task.

Example 1.1. The formula $|N_1 \cup N_2| = n_1 + n_2$ is valid if

a) Sets N_1 and N_2 contain $n_1 = |N_1|$ and $n_2 = |N_2|$ elements, respectively.
b) The sets have no elements in common $N_1 \cap N_2 = \emptyset$.

GENERALIZED SUM RULE

If the i^{th} of m tasks $1 \le i \le m$ can be performed in any of n_i ways, and if these cannot be performed at the same time, then there are $n_1 + n_2 + \cdots + n_m$ ways of performing any of the m tasks.

Example 1.2. The formula $\left|\bigcup_{i=1}^{m} N_i\right| = n_1 + n_2 + \cdots + n_m$ is valid if

a) m sets $N_1, N_2, \cdots, N_m$ contain $n_1 = |N_1|, n_2 = |N_2|, \cdots, n_m = |N_m|$ elements, respectively.
b) No pair of (distinct) sets N_i and N_j $(1 \le i < j \le m)$ has an element in common (*pairwise disjoint sets*) $N_i \cap N_j = \emptyset$.

If the m sets $N_1, N_2, \cdots, N_m$ are *not* pairwise disjoint, the sum $n_1 + n_2 + \cdots + n_m$ overcounts the size of $\bigcup_{i=1}^{m} N_i$. The *principle of inclusion-exclusion*, to be discussed in §1.8, provides the corrections.

PRODUCT RULE

If a procedure is composed of two tasks, the first can be performed in any of n_1 ways and thereafter, the second task in any of n_2 ways (perhaps depending on the outcome of the first task), then the total procedure can be performed in any of $n_1 \times n_2$ ways.

GENERALIZED PRODUCT RULE

If a procedure is composed of m tasks, the first can be performed in any of n_1 ways and the ith task can be performed in any of n_i ways (perhaps depending on the outcome of the first i outcomes), then the total procedure can be performed in any of $n_1 \times n_2 \times \cdots \times n_m$ ways.

Example 1.3. A sequence of letters that reads the same forward and backward is a palindrome[1]; for example, ABADABA is a palindrome and ABADABADO is not.

a) The number of 5- or 6-letter palindromes is (by the product rule) 26^3.
b) The number of 5- or 6-letter palindromes that do *not* contain the letter R (by the product rule) is (by the product rule) 25^3.
c) The number of 5- or 6-letter palindromes that do contain the letter R is $26^3 - 25^3$.
e) The number of 5- or 6-letter palindromes in which *no* letter is repeated (by the product rule) is (by the product rule) $26 \times 25 \times 24$.

Jenny Craig and Weight Watchers should note the following palindrome (with spaces deleted) created by the distinguished topologist Professor Peter Hilton during World War II:

DOC NOTE, I DISSENT. A FAST NEVER PREVENTS A FASTNESS, I DIET ON COD.

Example 1.4. A *bit string* of length n is an n-tuple $\underline{x} = (x_0, x_1, \cdots, x_{n-1})$ with $x_i \in \mathcal{Z}_2 = \{0, 1\}$ for $0 \le i < n$.

a) The number of bit strings of length n is (by the product rule) 2^n.
b) The number of bit strings of length $n \ge 4$ that start with 1100 is (by the product rule) 2^n.
c) The number of bit strings of length $n \ge 4$ that begin or end with 1 is (by the product rule) 2^{n-2}.
d) The number of bit strings of length $n \ge 2$ that begin or end with either 0 or 1 is (by the sum *and* product rules) $4 \times 2^{n-2}$.
e) The number of bit strings of length $n \ge 2$ in which the 4th or 8th bits is equal to 1 is (by the sum *and* product rules) $3 \times 2^{n-2}$.

1.2 MATHEMATICAL INDUCTION

In the sections that follow, we define various *couting functions*, to include permutation, combinations, and so forth. Often, we need to answer the question, "In how many ways can ···?" where ··· describes some property.

[1] From the Greek *palindromos*, meaning "running backward."

For example, various lotteries require the (hopeful) participant to choose n integers from 0 to 9, perhaps subject to some rules. What is the formula for the number of ways this can be done? Although no universal technique is available for solving such problems, mathematical induction may be successful to prove a formula, if the correct answer can be guessed. Several examples in this chapter will illustrate its usefulness.

Guiseppe Peano (1858–1932) studied mathematics at the University of Turin. He made many contributions to mathematics, and his most celebrated is the Peano axioms, which define the natural numbers $\mathcal{Z} = \{0, 1, \cdots\}$, the letter $\mathcal{Z}$ derived from the German *zahlen* for numbers. Why the adjective *natural*? Are there unnatural numbers? Numbers describing quantity arise naturally when we count things. The Babylonians, Egyptians, and Romans advanced the idea of using symbols to represent quantities. The Roman number system used symbols—X for 10, I for 1, and V for 5, and then incorporated the *place value system* in which XIV was the representation of 14.

Peano defined the natural numbers axiomatically; his fifth axiom

PA#5. A **predicate**[2] $\mathcal{P}$ defined on $n \in \mathcal{Z}$ is true for $n \in \mathcal{Z}$ if

— $\mathcal{P}(0)$ is true—the *base case*.
— the implication $\mathcal{P}(n) \rightarrow \mathcal{P}(n+1)$ is true for every $n \geq 0$—the *inductive step*.

This is referred to as the principle of mathematical induction.

Example 1.5. Prove

$$\sum_{i=1}^{n} i = \frac{1}{2} n(n+1) \quad 1 \leq n < \infty \tag{1.1}$$

Solution (by mathematical induction). $\mathcal{P}(n)$ is true for $n = 1$ because

$$\sum_{i=1}^{1} i = 1 = \frac{1}{2}(1 \times 2)$$

Assume $\mathcal{P}(n)$ is true; then equation (1.1) for $(n + 1)$ gives

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) = \frac{1}{2} n(n+1) + (n+1) \\ &= \frac{1}{2}(n+1)(n2) \end{aligned}$$

1.3 FACTORIAL

The factorial of a non-negative integer n is

[2] A *predicate* $\mathcal{P}$ on $\mathcal{Z}$ is a function defined on $\mathcal{Z}$ for which the value $\mathcal{P}(N)$ is either true or false.

$$n! = \begin{cases} 0 & \text{if } n = 0 \\ n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 & \text{if } n > 0 \end{cases} \tag{1.2a}$$

which may be written as

$$n! = n \times (n-1)! \quad n > 0 \quad 0! \equiv 1 \tag{1.2b}$$

The m-factorial of n is the product

$$(n)_m = \begin{cases} 1 & \text{if } m = 0 \\ n \times (n-1) \times (n-2) \times \cdots \times (n-m+1) & \text{if } 1 \le m \le n \\ 0 & \text{if } m > n \end{cases} \tag{1.3a}$$

We have the formula

$$(n)_m = \frac{n!}{(n-m)!} \quad 0 \le m \le n \tag{1.3b}$$

Table 1.1 gives the values of $n!$ for[3] $n = 1(1)14$.

Stirling's Formula (1730). Since $n!$ increases very rapidly with n, it is necessary to have a simple formula for large n. A derivation of the following asymptotic formula

$$n! \approx \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} \quad n \to \infty \tag{1.4a}$$

is given in [Feller 1957, pp. 50–53]. The meaning of the $\approx$ in equation (1.4*a*) is

$$1 = \lim_{n \to \infty} \frac{n!}{\sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n}} \tag{1.4b}$$

The following correction to equation (1.4*b*) is in [Feller 1957, p. 64].

$$n! \approx \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n+\frac{1}{12n}-\frac{1}{360n^3}} \quad n \to \infty \tag{1.4c}$$

Table 1.2 compares $n!$ and the approximation in equation (1.4*a*) for $n = 1(1)12$.

TABLE 1.1. n! for n = 1(1)14

n	n!	n	n!	n	n!	n	n!	n	n!
0	1	1	1	2	2	3	6	4	24
5	120	6	720	7	5040	8	40320	9	362880
10	3628800	11	39916800	12	479001700	13	6227020800	14	87178291200

[3]The table maker's notation $n = 1(1)12$ indicates the table contains entries for the parameter values $n = 1$ increasing in steps of 1 until $n = 14$.

TABLE 1.2. Comparison of $n!$ and Stirling, Approximation [Equation (1.4a)] for $n = 1(1)12$

n	n!	Equation (1.4a)	% Error
1	1	0.922137	7.786299
2	2	1.919004	4.049782
3	6	5.836210	2.729840
4	24	23.506175	2.057604
5	120	118.019168	1.650693
6	720	710.078185	1.378030
7	5040	4980.395832	1.182622
8	40320	39902.395453	1.035726
9	362880	359536.872842	0.921276
10	3628800	3598695.618741	0.829596
11	39916800	39615625.050577	0.754507
12	479001600	475687486.472776	0.691879

1.4 BINOMIAL COEFFICIENTS

The binomial coefficient sometimes displayed as $\binom{n}{m}$ and sometimes as $C(n, m)$ is defined for $n \geq 0$ by

$$\binom{n}{m} = \begin{cases} \dfrac{n!}{m!(n-m)!} & \text{if } 0 \leq m \leq n \\ 0 & \text{otherwise} \end{cases} \tag{1.5}$$

If $n \geq 0$ and $0 \leq m \leq n$, the negative binomial coefficient is defined by

$$\binom{-n}{m} = \frac{-n(-n-1)(-n-2)\cdots(-n-(m-1))}{m!} = (-1)^m \binom{n+m-1}{m} \tag{1.6}$$

Table 1.3 lists the binomial coefficients $\binom{n}{m}$ for $m = 0(1)n$ and $n = 0(0)10$.

In addition to his many contributions to mathematics, Blaise Pascal (1623–1662) invented the *Pascaline*, which is a digital calculator using 10-toothed gears to speed on arithmetic. Pascal observed an important recurrence connecting the entries in Table 1.3 and providing a natural way to extend it.

Theorem 1.1 (Pascal's triangle). $\binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1}$ for $0 \leq m \leq n$.

Proof. First, write

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{m+1}{n+1}\binom{n+1}{m+1}$$

TABLE 1.3. Binomial Coefficients $\binom{n}{m}$ with $m = 0(1)n$ and $n = 0(1)10$

	$m \rightarrow$										
$\downarrow n$	0	1	2	3	4	5	6	7	8	9	10
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		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

$$\binom{n}{m+1} = \frac{(n+1)!}{m!(n-m+1)!} = \frac{n-m}{n+1}\binom{n+1}{m+1}$$

Next, adding gives

$$\binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1} \quad \blacksquare$$

Pascal's observation led Isaac Newton (1642–1727) to discover the following theorem.

Theorem 1.2 (the binomial theorem). If $0 \le n < \infty$, then

$$(x+y)^n = \sum_{m=0}^{n} x^m y^{n-m} \binom{n}{m} \tag{1.7}$$

Proof. Using Pascal's triangle

$$\begin{aligned}
\sum_{m=0}^{n} x^m y^{n-m}\binom{n}{m} &= \sum_{m=0}^{n} x^m y^{n-m}\left[\binom{n-1}{m} + \binom{n-1}{m-1}\right] \\
&= y\sum_{m=0}^{n-1} x^m y^{n-1-m}\binom{n-1}{m} + x\sum_{m=1}^{n} x^{m-1} y^{n-1-(m-1)}\binom{n-1}{m-1} \\
&= y(x+y)^{n-1} + y(x+y)^{n-1} \\
&= (x+y)^n. \qquad \blacksquare
\end{aligned}$$

The analysis of many hashing protocols will involve expressions involving the binomial coefficients. A few useful identities are provided in the Appendix. A more

extensive collection may be found in [Gould 1972]. Incidentally, a mathematician could make a living just proving binomial coefficient identities. A search on Google on July 9, 2007 for binomial coefficients yielded 37,200 hits.

1.5 MULTINOMIAL COEFFICIENTS

We shall show in §1.6 that the binomial coefficient $\binom{n}{m}$ may be interpreted as

- The number of subsets of size m chosen from a universe $\mathcal{U}$ of size n.
- The number of ways of selecting a sample of m elements (objects) from a universe $\mathcal{U}$ of size n.

However, instead of only selecting a sample consisting of one kind from a universe of size n, we can partition the elements of $\mathcal{U}$ into k subsets $M_0, M_1, \cdots, M_{k-1}$ of sizes $m_0, m_1, \cdots, m_{k-1}$, where

$$m_i \geq 0 \quad 0 \leq i < k \quad n = m_0 + m_1 + \cdots + m_{k-1}$$

The *multinomial coefficient* is an extension of the binomial coefficient defined by

$$\binom{m}{m_0 m_1 \cdots m_{k-1}} = \frac{n!}{m_0!\, m_1! \cdots m_{k-1}!} \tag{1.8}$$

The analog of the binomial theorem is

Theorem 1.3 (the multinomial theorem). If $0 \leq n < \infty$, then

$$(x_0 + x_1 + \cdots + x_{k-1})^n = \sum_{\substack{m_0, m_1, \cdots, m_{k-1} \\ m_i \geq 0 \quad 0 \leq i \leq k \\ n = m_0 + m_1 + \cdots + m_{k-1}}} \prod_{i=0}^{k-1} x_i^{m_i} \binom{m}{m_0 m_1 \cdots m_{k-1}} \tag{1.9}$$

Proof. By induction on k. ■

1.6 PERMUTATIONS

An m-permutation from the universe $\mathcal{U}$ of n elements is an ordered sample $\underline{x} = (x_0, x_1, \cdots, x_{m-1})$ whose elements $\{x_i\}$ are in $\mathcal{U}$.

There are different flavors of permutations, as follows:

Permutations Without Repetition

$x_i = x_j \Leftrightarrow i = j$

Permutations With Unrestricted Repetition

$x_{i_0} = x_{i_1} = \cdots = x_{i_{s-1}}$ for s distinct indices $i_0, i_1, \cdots, i_{s-1}$ with *no* restriction on s or the indices $\{i_j\}$

Permutations With Restricted Repetition

$x_{i_0} = x_{i_1} = \cdots = x_{i_{s-1}}$ for s distinct indices $i_0, i_1, \cdots, i_{s-1}$ with *some* restrictions on s and/or the indices $\{i_j\}$

Theorem 1.4. The number of m-permutations from the universe $\mathcal{U}$ of n elements is n^m.

Proof. The product rule. ■

Example 1.6. The number of n-bit sequences $\underline{x} = (x_0, x_1, \cdots, x_{n-1})$ with $x_i \in \mathcal{Z}_2 = \{0, 1\}$ for $0 \le i < n$ is 2^n by the product rule.

Example 1.7. The American Standard Code for Information Interchange (ASCII) alphabet is a 7-bit code representing

- Uppercase and lowercase alphabetic characters `a b` ··· `z A B` ··· `Z`;
- Digits `0 1` ··· `9`;
- Blank space, punctuation `. , ! ? ;:` –;

Of the $128 = 2^7$ possible 7-bit sequences, only 95 are *printable*; the remaining 33 are nonprintable characters that consist mostly of control characters; for example,

- `BELL`, which rings a bell when the typewriter carriage returns—I hope everyone remembers what a typewriter is?[4]
- `CR` (or linefeed), which shifts the *cursor* to the next line

plus many communication control characters.

Theorem 1.5. The number $N_{n,m}(\neg\mathcal{R})$ of m-permutations without repetition from the universe $\mathcal{U}$ of n elements is $(n)m$.

Note in the special case $m = n$, the number of n-permutations without repetition from the universe $\mathcal{U}$ of n elements is $n!$.

Let $\mathcal{U} = \{0, 1, \cdots, n-1\}$ and suppose x is an n-permutations without repetition of the elements of $\mathcal{U}$. x can be interpreted as a rearrangement of the elements of $\mathcal{U}$, and the 2-rowed notation $\left(x = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ x_0 & x_1 & x_2 & \cdots & x_{n-1} \end{pmatrix} \right)$ is often used to emphasize this interpretation of x.

[4] My former employer used to manufacturer and sell typewriters; I believe they were assembled in Lexington, Kentucky. The *Selectric*, which was introduced in 1961, provided a convenient way to enter data into a computer. Various versions of the Selectric followed during the next 30 years. Finally in 1990, IBM formed a wholly owned subsidiary consolidating the company's typewriter, keyboard, intermediate and personal printers, and supplies business in the United States, including manufacturing and development facilities. IBM also reported that it was working to create an alliance under which Clayton & Dubilier, Inc. would become the majority owner of the new subsidiary and that IBM was studying a plan to include the remainder of its worldwide "information products" business in the alliance in the United States, including manufacturing and development facilities. A year later, IBM and Clayton & Dubilier, Inc. created a new information products company called Lexmark International, Incorporated to develop, manufacture, and sell personal printers, typewriters, keyboards, and related supplies worldwide.

When we interpret a permutation x as a rearrangement of the elements of $\mathcal{U}$, it is natural to compose or multiply them as follows:

$$x = (x_0, x_1, \cdots, x_{n-1}); \quad i \xrightarrow{x} x_i$$
$$y = (y_0, y_1, \cdots, y_{n-1}); \quad i \xrightarrow{y} y_i$$
$$x \times y \equiv z = (z_0, z_1, \cdots, z_{n-1}); \quad i \xrightarrow{x \times y} y_{x_i}$$

then the set of *all* $n!$ permutations of the elements of $\mathcal{U}$ forms a group[5] the symmetric group G_n. A transposition x is a permutation of the elements of $\mathcal{U}$, which leaves all of the elements alone other than elements i and j, which it interchanges. For example, if $i = 1, j = 4$, and $n = 8$, then

$$x = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 2 & 3 & 1 & 5 & 6 & 7 \end{pmatrix}$$

is a transposition.

The transpositions form the building blocks of the symmetric group G_n. The following theorem summarizes the basic properties that we will later use.

Theorem 1.6. For the symmetric group G_n.

a) A transposition x is *idempotent*, meaning $x \times x = 1$, where 1 is the identity permutation

$$1 = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ 0 & 1 & 2 & \cdots & n-1 \end{pmatrix}$$

b) Every permutation can be written, not necessarily in a unique way, as a product of transpositions; that is, the transpositions of $\mathcal{U}$ *generate* the symmetric group G_n.

c) If $x = y_0 \times y_1 \times \cdots \times y_{m-1} = y'_0 \times y'_1 \times \cdots \times y'_{m'-1}$, then m and m' are either even or odd.

The alternating group A_n of $\mathcal{U}$ consists of all permutations whose representation as a product of transpositions involving an *even* number of transpositions.

An m-permutation with repetition from the universe $\mathcal{U}$ of n elements is an ordered sample $\underline{x} = (x_0, x_1, \cdots, x_{m-1})$, whose elements $\{x_i\}$ are in $\mathcal{U}$ with no restriction on the number of times each element of $\mathcal{U}$ appears.

The term *sampling* in statistics refers to a process by which an m-permutation may be constructed. Imagine an urn that contains n balls bearing the numbers 0, 1,

[5]The elements $\{u\}$ of $\mathcal{U}$ form a group if
1. $u_1, u_2 \in \mathcal{U}$ implies $u_1 \times u_2 \in \mathcal{U}$ (closure).
2. $u_1, u_2, u_3 \in \mathcal{U}$ implies $u_1 \times (u_2 \times u_3) = (u_1 \times u_2) \times u_3$ (associativity law).
3. There exists an element $e \in \mathcal{U}$ such that $u \times e = e \times u = u$ for all $u \in \mathcal{U}$ (identity).
4. for every $u \in \mathcal{U}$, there exists an element $u^{-1} \in \mathcal{U}$ such that $u \times u^{-1} = u^{-1} \times u = e$ (inverse).

$\cdots, n-1$. A sampling process describes how the sample is constructed; two variants of sampling are worth noting, as follows:

Sampling without Replacement

After a ball is drawn from the urn (the person who draws the ball is of course blindfolded), its number is recorded and the ball is not returned to the urn.

Sampling with Replacement

After a ball is drawn from the urn (same security provisions as before), its number is recorded and the ball is returned to the urn.

Frequently, the ball manufacturers insist on business, and the urn contains N replicas of each numbered ball.

Example 1.8 (Powerball). His truck broke down the morning he and his wife of 20 years discovered they had won a $105.8 million Powerball jackpot from June 27th. Powerball is an American lottery operated by the Multi-State Lottery Association (MUSL), a consortium of lottery commissions in 29 states, the District of Columbia, and the U.S. Virgin Islands. Powerball is licensed as the monopoly provider of multistate lotteries in these jurisdictions.

A player picks 5 numbers from 1 to 55 and one number from 1 to 42.

Every Wednesday and Saturday night at 10:59 p.m. Eastern time, the Powerball management draws 5 white balls out of a drum with 55 balls and 1 red ball out of a drum with 42 red balls. Five balls from 53 plus 1 power ball from a separate group of 42 are selected. First prize is won by matching all 6 balls drawn. There are nine prize levels.

This process demonstrates sampling without replacement.

There are many varieties of permutations with specified repetition, for example, specifying the number of repetitions m_i of the universe $\mathcal{U}$ element a_i subject to the obvious conditions

$$m_i \geq 0 \quad m = m_0 + m_1 + \cdots + m_{n-1}$$

Theorem 1.7. The number $N_{n,\underline{m}}(\mathcal{R})$ of m-permutations from $\mathcal{U} = \{0, 1, \cdots, n-1\}$ with the specified repetition pattern $\underline{m} = (m_0, m_1, \cdots, m_{n-1})$ is

$$N_{n,m}(\mathcal{R}) = \binom{m}{m_0 m_1 \cdots m_{n-1}} = \frac{m!}{m_0!\, m_1! \cdots m_{n-1}!} \tag{1.10}$$

Example 1.9. How many ways are there of permutating the letters of CALIFORNIA?

Answer. $\dfrac{12!}{3!2!} = 11!$ ■

Example 1.10. I gave the following problem during the recall election for the Governor of California when I taught discrete mathematics at the University of California at Santa Barbara in the fall of 2003.

Which of the two names GRAYDAVIS or ARNOLDSCHWARZENEGGER has the most permutations?

Answer. There are

$$N_{GD} = \binom{9}{2} = 181\,440$$

permutations of the letters of GRAYDAVIS because only the letter A is repeated and

$$N_{AS} = \binom{20}{2\,3\,2\,3\,2} = 1\,550\,400 \times 13!$$

of the letters of ARNOLDSCHWARZENEGGER because the letters A and G each occur twice and the letters R and E each occur three times. ■

And the winner was Arnold Schwarzenegger. I am reasonably certain this question did not affect the outcome.

Other types of restrictions on repetitions are possible.

Example 1.11. How many permutations are there of MASSACHUSETTS in which no S's are adjacent?

Answer. There are $\binom{9}{1\,2\,1\,1\,1\,1\,2}$ permutations of MAACHUETT. It remains to place the 4 Ss, one in each of the positions between, before, or after the letters in MAACHUETT, for example, as shown by ↑ in

↑ M ↑ A ↑ A ↑ C ↑ H ↑ U ↑ E ↑ T ↑ T ↑

These four positions may be chosen from the 10 ↑s (without repetition) in $\binom{10}{4}$ ways. ■

1.7 COMBINATIONS

An m-combination from the universe $\mathcal{U}$ of n elements is an unordered sample $\{x_0, x_1, \cdots, x_{m-1}\}$ whose elements $\{x_i\}$ are in $\mathcal{U}$.

Note that we have written $\{x_0, x_1, \cdots, x_{r-1}\}$ rather than $(x_0, x_1, \cdots, x_{r-1})$ because an *ordering* is implicit in the latter.

Theorem 1.8. The number of m-combinations from the universe $\mathcal{U}$ of n elements is $\binom{n}{m}$.

Just as in the case of permutations, there are combinations with additional constraints; two are mentioned here.

Example 1.12. How many permutations are there of the 15 letters of POLYUNSATURATED maintaining the relative order of the vowels A, E, I, O, and U?

Solution.

1. The positions in which the vowels OUAUAE appearing in POLYUNSATURATED can be chosen is $\binom{15}{6}$.
2. Having chosen their positions, their orders are determined.
3. There remain $\binom{9}{1\,1\,1\,1\,1\,2\,1\,1} = 181\,400$ permutations of the remaining letters of PLYNSTRTD. ■

A is a multiset of size m of a universe $\mathcal{U}$ with n elements if it contains m_i copies of the element $a_i \in \mathcal{U}$ for $0 \le i < k$. We can write

$$A = \{(a_0)_{\ell_0}, (a_1)_{\ell_1}, \cdots (a_{m-1})_{\ell_{m-1}}\}$$

where the elements $a_0, a_1, \cdots, a_{m-1}$ of $\mathcal{U}$ are distinct and

$$\ell_i \ge 0 \quad 0 \le i < m \quad n = \ell_0 + \ell_1 + \cdots + \ell_{m-1}$$

A multiset can also be interpreted as an ordered permutation with specified repetition, equivalently, an ordered partition[6] of the integer n into m non-negative parts.

To count the number $C_{n,m}$, we consider a set of $n + m - 1$ positions (horizontal lines) corresponding to the n elements of $\mathcal{U}$ together with $m - 1$ *fictitious* elements. We place a divider (a vertical line) in the following locations:

- Immediately to the left of the leftmost position
- Immediately to the right of the leftmost position
- $m - 1$ dividers through some $m - 1$ of the $n + m - 1$ positions

The partition is determined by dividing the set $\{0, 1, \cdots, n - 1\}$ according to the number of positions between dividers (Figure 1.1).

Theorem 1.9. The number $C_{n,m}$ of partitions of the integer n into m non-negative parts is $\binom{n+m-1}{m-1} = \binom{n+m-1}{n}$.

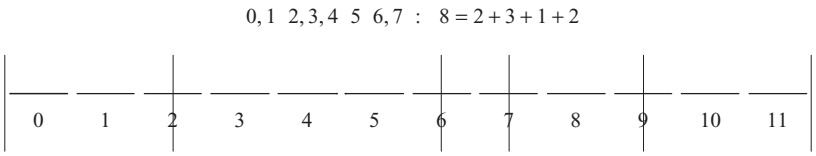


Figure 1.1. An ordered partition of $n = 8$ into $m = 4$ parts.

[6] See *Example 2.6* in Chapter 2 for another type of partition.

Corollary 1.10. The number $C_{n,m}$ of partitions of the integer n into m positive parts is $\binom{n-1}{m-1}$.

Proof. If

$$\ell_i \geq 0 \quad 0 \leq i < m \quad n = \ell_0 + \ell_1 + \cdots \ell_{m-1} \tag{1.11a}$$

then $\ell^* = (\ell_0^*, \ell_1^*, \cdots, \ell_{m-1}^*)$ defined by

$$\ell_i^* = \ell_i + 1 \quad 0 \leq i < m \tag{1.11b}$$

implies (1.11*c*)

$$\ell_i^* > 0 \quad 0 \leq i < m \quad n - m = \ell_0^+ \ell_1^* + \cdots \ell_{m-1}^* \tag{1.11c}$$

and conversely, if $\underline{l}$ and $\underline{l}^*$ are related by equation (1.11*b*), then the conditions of equation (1.11*b*) imply the conditions of equation (1.11*a*). ■

Example 1.13 (donuts). Dunkin' Donuts offers more than 30 varieties of donuts, including the ever popular chocolate creme-filled donut.[7]

How many ways are there of buying 12 donuts from the 30 varieties without any restriction on the number of each kind?

Solutions. $\binom{29+12}{29}$

How many ways are there of buying 12 donuts from the 30 varieties if at least four must be of one specific variety?

Solutions. Suppose the desired donut is of the 0th variety. Equation (1.11*a*) is replaced by

$$\ell_i \begin{cases} \geq 4 & \text{if } i = 0 \\ \geq 9 & \text{if } 0 < i < 30 \end{cases} \qquad 12 = \ell_0 + \ell_1 + \cdots \ell_{29}$$

If we set

$$\ell_i^* = \begin{cases} \ell_i - 4 & \text{if } i = 0 \\ \ell_i & \text{if } 0 < i < 30 \end{cases}$$

[7] I worked at the Puzzle Palace during the summer of 1997. While on this assignment, I violated one of the security rules by failing to turn off my workstation monitor after a logout. The NSA logo remained there for all to see—of course, only those who were cleared to enter the facility could see it! Nevertheless, there was a punishment; I had to buy a dozen donuts for my group after I was told the next day of my infraction, and I was further informed that the *Chief* preferred the chocolate creme-filled variety. I did what I had to do!

then

$$\ell_i^* \geq 0 \quad 0 \leq i < 30 \quad 8 = \ell_0 + \ell_1 + \cdots \ell_{29}$$

yielding the answer is $\binom{29+8}{29}$.

1.8 THE PRINCIPLE OF INCLUSION-EXCLUSION

Let $N_0, N_1, \cdots, N_{n-1}$ be sets in some universe $\mathcal{U}$. Then

$$|N_0 \cup N_1| = |N_0| + |N_1| - |N_0 \cap N_1| \tag{1.12a}$$

$$|N_0 \cup N_1 \cup N_2| = |N_0| + |N_1| + |N_2| - |N_0 \cap N_1| - |N_0 \cap N_2| - |N_1 \cap N_2| + |N_0 \cap N_1 \cap N_2| \tag{1.12b}$$

Note that

- A point $u \in N_0$ is counted once on the right-hand side of equation (1.12a) [1 = 1 + 0 − 0] if $u \neq N_1$.
- A point $u \in N_0$ is also counted once on the right-hand side of equation (1.12a) [1 = 1 + 1 − 1] if $u = N_1$.

Similarly,

- A point $u \in N_0$ is counted once on the right-hand side of equation (1.12b) [1 = 1 + 0 + 0 − 0 − 0 − 0 + 0] if $u \neq N_1$ and $u \neq N_2$.
- A point $u \in N_0$ is also counted once on the right-hand side of equation (1.12b) [1 = 1 + 1 + 0 − 1 − 0 − 0 − 0 or 1 = 1 + 0 + 1 − 0 − 1 − 0 − 0] if $u = N_1$ and $u \neq N_2$ or $u = N_2$ and $u \neq N_1$.
- A point $u \in N_0$ is also counted once on the right-hand side of equation (1.12b) [1 = 1 + 1 + 1 − 1 − 1 − 1 + 1] if $u = N_1$ and $u = N_2$.

These equalities are special cases of the following theorem.

Theorem 1.11 (principle of inclusion-exclusion). If $N_0, N_1, \cdots, N_{n-1}$ are sets in a universe $\mathcal{U}$, then

$$\left|\bigcup_{i=0}^{n-1} N_i\right| = \sum_{i=0}^{n-1} |N_i| - \sum_{0 \leq i_0 < i_1 < n} |N_{i_0} \cap N_{i_1}| + \sum_{0 \leq i_0 < i_1 < i_2 < n} |N_{i_0} \cap N_{i_1} \cap N_{i_2}| \cdots (-1)^{n-1} |N_0 \cap N_1 \cap \cdots \cap N_{n-1}| \tag{1.13}$$

Proof. By mathematical induction using the equality in equation (1.12a). ■

Sometimes the enumeration combines the use of both ordered permutations and the principle of inclusion-exclusion.

Example 1.14 (more donuts). In how many ways can 27 donuts be chosen from the 30 varieties if *fewer* than 10 of the 0th variety is to be included?

Solution. Equation (1.11*a*) is now replaced by

$$\ell_i \begin{cases} < 10 & \text{if } i = 0 \\ \geq 9 & \text{if } 0 < i < 30 \end{cases} \qquad 27 = \ell_0 + \ell_1 + \cdots \ell_{29} \tag{1.14a}$$

The complementary problem is

$$\ell_i \begin{cases} \geq 10 & \text{if } i = 0 \\ \geq 9 & \text{if } 0 < i < 30 \end{cases} \qquad 27 = \ell_0 + \ell_1 + \cdots \ell_{29} \tag{1.14b}$$

If we set

$$\ell_i^* = \begin{cases} \ell_i - 10 & \text{if } i = 0 \\ \ell_i & \text{if } 0 < i < 30 \end{cases}$$

then

$$\ell_i^* \geq 0 \quad 0 \leq i < 30 \quad 18 = \ell_0 + \ell_1 + \cdots \ell_{29}$$

which has $\binom{29+18}{29}$ solutions, which means the original problem equation (1.14*a*) has

$$\binom{29+28}{29} - \binom{29+18}{29}$$

solutions. ■

1.9 PARTITIONS

A partition[8] Π of a set of n elements, say $\mathcal{Z}_n = \{0, 1, \cdots, n-1\}$, is a collection of nonempty sets whose union is $\mathcal{Z}_n$. For example, the five partitions of $\mathcal{Z}_3$ are

$$\Pi_1 : \{0\}\{1\}\{2\} \quad \Pi_2 : \{0,1\}\{2\} \quad \Pi_3 : \{0,2\}\{1\} \quad \Pi_4 : \{1,2\}\{0\} \quad \Pi_6 : \{0,1,2\}$$

The number of partitions of $\mathcal{Z}_n$ is the Bell number B_n. *Example 2.6* in Chapter 2 asks the reader to derive the recursion

$$B_{n+1} = \binom{n}{0} B_0 + \binom{n}{1} B_1 + \cdots + \binom{n}{n} B_n \quad 0 \leq n < \infty; B_0 = 1, B_2 = 1 \tag{1.15}$$

and the generating functions of the $\{B_n\}$.

[8] In §1.6 we defined the ordered partition; without the prefix *order*, the order of the elements in a set in Π and the order in which these sets are listed in Π are both immaterial.

The Stirling number (of the second kind) $S_{n,k}$ is the number of partitions of $\mathcal{Z}_n$ into k (nonempty) sets; thus,

$$S_{3,1} = 1 \quad S_{3,2} = 3 \quad S_{3,3} = 1$$

The Stirling numbers (of the second kind) $\{S_{n,k}\}$ are obviously related to the Bell numbers $\{B_n\}$ by

$$B_n = \sum_{k=1}^{n} S_{n,k} \tag{1.16}$$

A proof of the formula below will be given in Chapter 2.

$$S_{n,k} = \frac{1}{k!} \sum_{s=0}^{k} \binom{k}{s} (-1)^s (k-s)^n \tag{1.17}$$

There is an extensive literature dealing with Stirling numbers, which arise in many applications; see, for example, [Bleick and Wang 1974]. We will encounter the $\{S_{n,k}\}$ in Chapter 10.

1.10 RELATIONS

A relation ~ on a yset X generalizes the notion of function specifying some collection of pairs (x, y), and we write $x \sim y$ for $x, y \in X$ read (elements) *x and y are related* and $x \not\sim y$, if they are not related.

A partition $X_0, X_1, \cdots$ of a set X as in §1.9 determines a relation ~ by the rule $x \sim y$ if and only if $x, y \in X_i$ for some i.

Conversely, a relation ~ on a set X determines a partition $X_0, X_1, \cdots$ in which

- X_i consists of ~-related elements.
- If $x \in X_i$, $y \in X_j$ and $i \neq j$, then $x \not\sim y$.

The following properties may or not be enjoyed by a relation ~:

1. ~ is *reflexive* if $x \sim x$; ~ is *irreflexive* if $x \not\sim x$.
2. ~ is *symmetric* if $x \sim y$ implies $y \sim s$; a reflexive relation ~ is *asymmetric* if $x \sim y$ and $y \sim x$ can only occur if $y = x$.
3. ~ is *transitive* if $x \sim y$ and $y \sim z$ implies $x \sim z$; ~ is *intransitive* if $x \sim y$ and $y \sim z$ implies $x \not\sim z$.

In addition to the modifiers *ir*, *anti*, and *in*, there are definitions for the modifier **not** as in *not* reflexive, *not* symmetric, and *not* transitive; we leave to the reader's creativity, their definitions.

~ is an **equivalence relation** if it is reflexive, symmetric, and transitive.

1.11 INVERSE RELATIONS

The binomial coefficients can be used to define a sort of transformation on sequences; for example,

$$a = (a_0, a_1, \cdots) \to b = (b_0, b_1, \cdots)$$
$$b_n = \sum_l (-1)^k \binom{n}{k} a_k \quad n = 0, 1, \cdots \tag{1.18a}$$

Theorem 1.12. If equation (1.18*a*) holds, then

$$a_n = \sum_l (-1)^k \binom{n}{k} v_k \quad n = 0, 1, \cdots \tag{1.18b}$$

Solution: Start with the identity E8 in the Chapter 1 Appendix that follows, setting $b_n = (-1)^m \binom{m}{n}$. ■

Theorem 1.12 is one of many inverse relations (see [Riordan 1968]); we will use it in Chapter 10.

APPENDIX 1

Summations Involving Binomial Coefficients

Equations **E1** through **E8** follow easily from the binomial theorem

$$(x+y)^n = \sum_{m=0}^{n} x^m y^{n-m} \binom{n}{m}$$

and derivatives of it by evaluating for special values of x, y. ■

E1. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

E2. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^n \binom{n}{n} = 0$

E3. $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1}$

E4. $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$

E5. $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}$

E6. $\binom{n}{1} - 2\binom{n}{2} + 3\binom{n}{3} - \cdots + (-1)^n n\binom{n}{n} = 0$

E7. $2\binom{n}{2} + 6\binom{n}{3} + 12\binom{n}{4} + \cdots + n(n-1)\binom{n}{n} = n(n-1)2^{n-2}$

E8. $\sum_k (-1)^{k+m}(-1)^k \binom{n}{k}\binom{k}{m} = \delta_{n,m} = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{otherwise} \end{cases}$

E9. $\binom{n+m}{k} = \sum_{j=0}^{n} \binom{n}{j}\binom{m}{k-j}$

Vandermonde's Identity E9 is proved by counting the ways of choosing k elements from the set $A \cup B$, where $A \cap B = \emptyset$, A contains n, and B contains m elements.

$$\textbf{E10.}\quad \sum_{r=1}^{m} \frac{\binom{m}{r}}{\binom{n}{r}} = \frac{m}{n-m+1}$$

E10 is a special case of the formula

$$\sum_{r=j}^{k} \binom{m}{r} \Big/ \binom{n}{r} = (n+1)/(n-m+1)\left\{ \binom{m}{j} \Big/ \binom{n+1}{j} - \binom{m}{k+1} \Big/ \binom{n+1}{k+1} \right\}$$

contained in [Gould 1972, p. 46]. It may be proved by recognizing the identity

$$\binom{m}{r} \Big/ \binom{n}{r} = m/n \binom{m-1}{r-1} \Big/ \binom{n-1}{r-1}$$

$$\textbf{E11.}\quad x^{-1}(x+y+na)^n = \sum_{j=0}^{n} \binom{n}{j} (x+ja)^{j-1} \left(y+(n-j)a\right)^{n-j}$$

E11 is a nontrivial generalization of the Binomial theorem from Niel Henrik Abel (1802–1829) published in 1826 (see [Riordan 1968]). Abel is famous for proving the impossibility of representing a solution of a general equation of fifth degree or higher by a radical expression.

REFERENCES

W. W. Bleick and P. C. C. Wang, "Asymptotics of Stirling Numbers of the Second Kind", *Proceedings of the American Mathematical Society*, **42**, #2, pp. 575–580, 1974.

W. Feller, *An Introduction to Probability Theory and Its Applications*, Volume 1 (Second Edition), John Wiley & Sons (New York), 1957; (Third Edition), John Wiley & Sons (New York), 1967.

H. W. Gould, *Combinatorial Identities*, Henry W. Gould (Morgantown, West Virginia), 1972.

J. Riordan, *Combinatorial Identities*, John Wiley & Sons (New York), 1968.

K. H. Rosen, *Discrete Mathematics and Its Applications*, McGraw-Hill (New York), 2003.