Chapter 7

The Principle of Inclusion and Exclusion

7.1 THE PRINCIPLE AND SOME OF ITS APPLICATIONS

7.1.1 Some Simple Examples

In this chapter we introduce still another basic counting tool, known as the principle of inclusion and exclusion. We introduce it with the following example.

Example 7.1 Job Applicants Suppose that in a group of 18 job applicants, 10 have computer programming expertise, 5 have statistical expertise, and 2 have both programming and statistical expertise. How many of the group have neither expertise? To answer this question we draw a Venn diagram such as that shown in Figure 7.1.[1] There are 18 people altogether. To find out how many people have neither expertise, we want to subtract from 18 the number having programming expertise (10) and the number having statistical expertise (5). However, we may have counted several people twice. In particular, all people who have both kinds of expertise (the number of people in the intersection of the two sets programming expertise and statistical expertise in Figure 7.1) have been counted twice. There are 2 such people. Thus, we have to add these 2 back in to obtain the right count. Altogether, we conclude that

$$18 - 10 - 5 + 2 = 5$$

is the number of people who have neither expertise. We shall generalize the reasoning we have just gone through. ■

[1] The reader who is unfamiliar with Venn diagrams should consult any finite mathematics text, for example, Goldstein, Schneider, and Siegel [2001] or Mizrahi and Sullivan [1999].

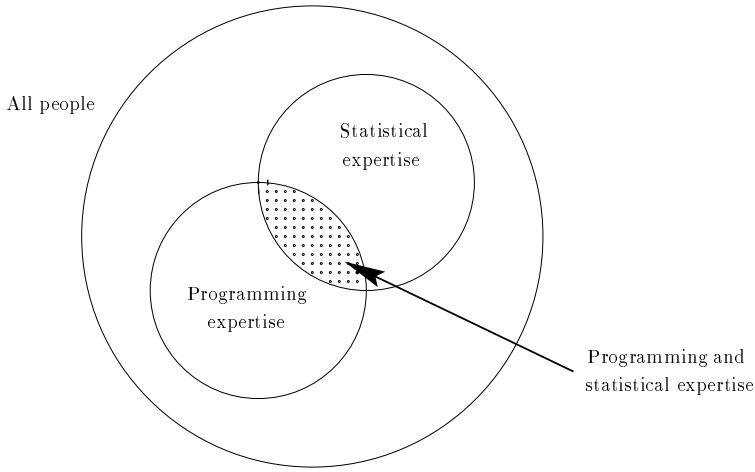


Figure 7.1: A Venn diagram for Example 7.1.

Suppose that we have a set A of N objects. Let $a_1, a_2, \ldots, a_r$ be a set of properties the objects may have, and let $N(a_i)$ be the number of objects having property a_i. An object may have several (or none) of the properties in question. Let $N(a_i')$ count the number of objects not having the property a_i. Hence, we have

$$N = N(a_i) + N(a_i').$$

Since an object can have more than one property, it is useful to count the number of objects having both properties a_i and a_j. This will be denoted by $N(a_i a_j)$. The number of objects having neither of the properties a_i and a_j will be denoted $N(a_i' a_j')$ and the number of objects having property a_j but not property a_i will be denoted $N(a_i' a_j)$. We shall also use the following notation, which has the obvious interpretation:

$$N(a_i a_j \cdots a_k),$$
$$N(a_i' a_j' \cdots a_k'),$$
$$N(a_i' a_j \cdots a_k),$$
$$\text{etc.}$$

In Example 7.1 the objects in A are the 18 people, so $N = 18$. Let property a_1 be having programming expertise and property a_2 be having statistical expertise. Then

$$N(a_1) = 10, \quad N(a_2) = 5, \quad N(a_1 a_2) = 2.$$

By computation, we determined that

$$N(a_1' a_2') = 5.$$

It is also possible to compute $N(a_1' a_2)$ and $N(a_1 a_2')$. The former is the number of people who have statistical expertise but do not have programming expertise, and this is given by $5 - 2 = 3$.

Our computation in Example 7.1 used the following formula for $N(a_1'a_2')$:

$$N(a_1'a_2') = N - N(a_1) - N(a_2) + N(a_1a_2). \tag{7.1}$$

Note that certain objects are *included* too often, so some of these have to be *excluded*. Equation (7.1) is a special case of a principle known as the *principle of inclusion and exclusion*. The process of including and excluding objects corresponds to the addition and subtraction, respectively, in Equation (7.1). Let us develop a similar principle for $N(a_1'a_2'a_3')$, the number of objects having neither property a_1 nor property a_2 nor property a_3. The principle is illustrated in the Venn diagram of Figure 7.2. We first include all the objects in A (all N of them). Then we exclude those having property a_1, those having property a_2, and those having property a_3. Since some objects have more than one of these properties, we need to add back in those objects which have been excluded more than once. We add back in (include) those objects having two of the properties, the objects corresponding to areas in Figure 7.2 that are colored in. Then we have added several objects back in too often, namely those which have all three of the properties, the objects in the one area of Figure 7.2 that has crosshatching. These objects must now be excluded. The result of this reasoning, which we shall formalize below, is the following formula:

$$\begin{aligned} N(a_1'a_2'a_3') \;=\; & N - N(a_1) - N(a_2) - N(a_3) + N(a_1a_2) + \\ & N(a_1a_3) + N(a_2a_3) - N(a_1a_2a_3). \end{aligned} \tag{7.2}$$

In general, the formula for the number of objects not having any of r properties is obtained by generalizing Equation (7.2). The general formula is called the *principle of inclusion and exclusion*. In the form we present it, the principle was discovered by Sylvester in the mid-nineteenth century. In another form, it was discovered by De Moivre [1718] some years earlier. The principle is given in the following theorem:

Theorem 7.1 (Principle of Inclusion and Exclusion) If N is the number of objects in a set A, the number of objects in A having none of the properties $a_1, a_2, \ldots, a_r$ is given by

$$\begin{aligned} N(a_1'a_2'\cdots a_r') \;=\; & N \;-\; \sum_i N(a_i) \;+\; \sum_{i\neq j} N(a_ia_j) \;- \\ & \sum_{\substack{i,j,k \\ \text{different}}} N(a_ia_ja_k) \;\pm\; \cdots \;+\; (-1)^r N(a_1a_2\cdots a_r). \end{aligned} \tag{7.3}$$

In (7.3), the first sum is over all i from $\{1, 2, \ldots, r\}$. The second sum is over all unordered pairs $\{i, j\}$, with i and j from $\{1, 2, \ldots, r\}$ and $i \neq j$. The third sum is over all unordered triples $\{i, j, k\}$, with i, j, and k from $\{1, 2, \ldots, r\}$ and i, j, k distinct. The general term is $(-1)^t$ times a sum of terms of the form $N(a_{i_1}a_{i_2}\cdots a_{i_t})$, where the sum is over all unordered t-tuples $\{i_1, i_2, \ldots, i_t\}$ from $\{1, 2, \ldots, r\}$, with $i_1, i_2, \ldots, i_t$ distinct. In the remainder of this chapter, we present applications and variants of the principle of inclusion and exclusion. We present a proof of Theorem 7.1 in Section 7.1.2.

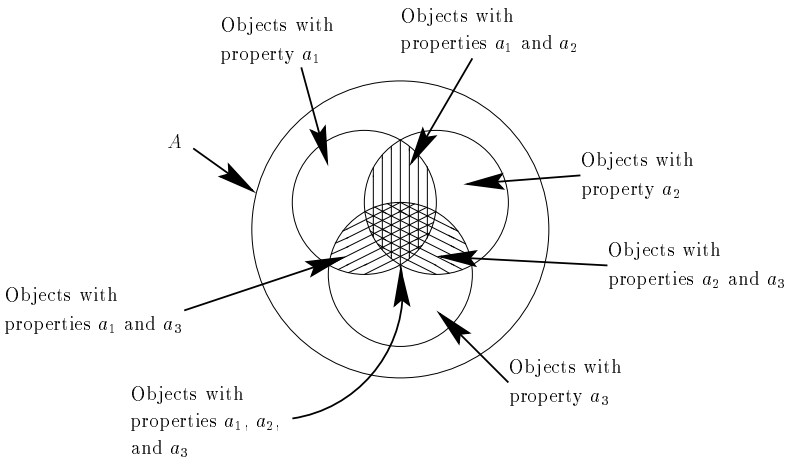


Figure 7.2: A Venn diagram illustrating the principle of inclusion and exclusion.

Example 7.2 Emissions Testing Fifty cars are tested for pollutant emissions of nitrogen oxides (NO_x), hydrocarbons (HC), and carbon monoxide (CO). One of the cars exceeds the environmental standards for all three pollutants. Three cars exceed them for NO_x and HC, two for NO_x and CO, one for HC and CO, six for NO_x, four for HC, and three for CO. How many cars meet the environmental standards for all three pollutants? We let A be the set of cars, let a_1 be the property of exceeding the standards for NO_x and let a_2 and a_3 be the same property for HC and CO, respectively. We would like to calculate $N(a_1'a_2'a_3')$. We are given the following information:

$$\begin{aligned} N &= 50, & N(a_1a_2a_3) &= 1, & N(a_1a_2) &= 3, & N(a_1a_3) &= 2, \\ N(a_2a_3) &= 1, & N(a_1) &= 6, & N(a_2) &= 4, & N(a_3) &= 3. \end{aligned}$$

Thus, by the principle of inclusion and exclusion,

$$N(a_1'a_2'a_3') = 50 - 6 - 4 - 3 + 3 + 2 + 1 - 1 = 42. \qquad \blacksquare$$

7.1.2 Proof of Theorem 6.1[2]

The idea of the proof of Theorem 7.1 is a very simple one. The left-hand side of (7.3) counts the number of objects in A having none of the properties. We shall simply show that every object having none of the properties is counted exactly one time in the right-hand side of (7.3) and every object having at least one property is counted exactly zero times (in a net sense). Suppose that an object has none of the properties in question. Then it is counted once in computing N, but not in $\sum N(a_i)$, $\sum N(a_ia_j)$, and so on. Hence, it is counted exactly once in the right-hand

[2] This subsection may be omitted. However, the reader is urged to read it.

side of (7.3). Suppose that an object has exactly p of the properties $a_1, a_2, \ldots, a_r$, $p > 0$. Now the object is counted $1 = \binom{p}{0}$ times in computing N, the number of objects in A. It is counted once in each expression $N(a_i)$ for a property a_i it has, so exactly $p = \binom{p}{1}$ times in $\sum N(a_i)$. In how many terms $N(a_i a_j)$ is the object counted? The answer is it is the number of pairs of properties a_i and a_j which the object has, and this number is given by the number of ways to choose two properties from p properties, that is, by $\binom{p}{2}$. Thus, the object is counted exactly $\binom{p}{2}$ times in $\sum N(a_i a_j)$. Similarly, in $\sum N(a_i a_j a_k)$ it is counted exactly $\binom{p}{3}$ times, and so on. All together, the number of times the object is counted in the right-hand side of (7.3) is given by

$$\binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \binom{p}{3} \pm \cdots + (-1)^r \binom{p}{r}. \tag{7.4}$$

Since $p \leq r$ and since by convention $\binom{p}{k} = 0$ if $p < k$, (7.4) becomes

$$\binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \binom{p}{3} \pm \cdots + (-1)^p \binom{p}{p}. \tag{7.5}$$

Since $p > 0$, Theorem 2.9 implies that the expression (7.5) is 0, so the object contributes a net count of 0 to the right-hand side of (7.3). This completes the proof.

7.1.3 Prime Numbers, Cryptography, and Sieves

One of the earliest problems about numbers to interest mathematicians was the problem of identifying all *prime numbers*, integers greater than 1 whose only positive divisors are 1 and themselves. Recently, Agrawal, Kayal, and Saxena [2002] presented a deterministic polynomial-time algorithm that determines whether a given integer $n > 1$ is prime or *composite* (nonprime). Previously, only nonpolynomial time algorithms, polynomial-time algorithms assuming well-known conjectures, and probabilistic algorithms were available to test whether a number is prime or composite. For example, if not identified as composite by a probabilistic test, a number is highly likely to be prime, i.e., an *industrial-grade prime*. This designation is an important one since prime numbers are needed in many practical applications and industrial-grade primes have been used. For more on these methods of primality testing, see Adleman and Huang [1992], Adleman, Pomerance, and Rumely [1983], Goldwasser and Kilian [1986], Miller [1976], Rabin [1980], or Solovay and Strassen [1977].

One critical use is in *cryptography*, the field of the mathematical sciences devoted to concealing messages. Nowadays, cryptography arises in problems such as keeping email secure, protecting the privacy of medical records, protecting the integrity

of electronic financial transactions, and protecting copyrights in a digital world. For example, it is well known that every positive integer greater than 1 can be uniquely factored as a product of primes. This is a key to the most commonly used "public-key" algorithm in cryptography, the *RSA Algorithm* due to Rivest, Shamir, and Adleman [1978]. Factoring integers has long been considered a hard computational problem. It is widely believed that integers cannot be factored in time polynomial in the number of bits or digits that represent the number. So widely is this believed that the security of cryptography methods such as RSA rely on the difficulty of factoring. One of the cornerstones of basing a cryptographic method on the hardness (i.e., nonpolynomial time) of a problem is that the definition of what it is possible to compute in polynomial time is independent of the model of computing used. Quantum computing, using devices based on quantum mechanics, is one such model. Quantum computers do not operate like conventional ones, but make use of the quantum states of atoms, which offers a computing capacity far in excess of current parallel supercomputers. However, only prototypes of these computers currently exist. Shor [1997] proved the remarkable result that a number can be factored in polynomial time in the quantum computing model. He obtained a similar result for the discrete log problem which is the basis of another cryptography method, Diffie-Hellman (see Diffie and Hellman [1976]). Thus, for problems of very practical interest, the quantum model has significantly faster algorithms than are known for the traditional computing models. These results not only demonstrated that quantum computing could give new power to computing, but also cast doubt on the safety of cryptography based on the hardness of factoring or discrete log. (For more on cryptography, see Anshel, Anshel, and Goldfeld [1999], Koblitz [1994], Rhee [1993], Schneier [1995], Seberry and Pieprzyk [1989], or Stallings [1999].) We return to cryptography in Section 9.2.5 and in particular to the RSA cryptosystem in Section 9.3.2.

An old problem in mathematics is to identify all prime numbers. The Greek Erastothenes is credited with inventing the following procedure for identifying all prime numbers between 1 and N. First write out all the numbers between 1 and N. Cross out 1. Then cross out those numbers divisible by and larger than 2. Search for the first number larger than 2 not yet crossed out—it is 3—and cross out all those numbers divisible by and larger than 3. Then search for the first number larger than 3 not yet crossed out—it is 5—and cross out all numbers divisible by and larger than this number; and so on. The prime numbers are the ones remaining when the procedure ends. The following shows the steps in this procedure if $N = 25$:

1. Cross out 1 and cross out numbers divisible by and larger than 2:

   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25

2. Cross out numbers divisible by and larger than 3 among those not yet crossed out:

   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25

3. Cross out numbers divisible by and larger than 5 among those not yet crossed out:

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

Dividing by 7, 11, and so on, does not remove any more numbers, so the numbers remaining are the prime numbers between 1 and 25. This procedure used to be carried out on a wax tablet (Vilenkin [1971]), with numbers punched out rather than crossed out. The result was something like a sieve, and hence the procedure came to be known as the *Sieve of Erastothenes*. A basic question that arises is: How many primes are there between 1 and N? The answer is closely related to the answer to the following question: How many numbers between 1 and N (other than 1) are not divisible by 2, 3, 5, ...? In the next example, we see how to answer questions of this type.

Example 7.3 How many integers between 1 and 1000 are:

(a) Not divisible by 2?
(b) Not divisible by either 2 or 5?
(c) Not divisible by 2, 5, or 11?

To answer these questions, let us consider the set of 1000 integers between 1 and 1000 and let a_1 be the property of being divisible by 2, a_2 the property of being divisible by 5, and a_3 the property of being divisible by 11. We would like the following information:

$$\text{(a) } N(a_1'); \quad \text{(b) } N(a_1'a_2'); \quad \text{(c) } N(a_1'a_2'a_3').$$

We are given $N = 1000$. Also,

$$N(a_1) = 500,$$

since every other integer is divisible by 2. Hence,

$$N(a_1') = N - N(a_1) = 500,$$

which gives us the answer to (a). Next,

$$N(a_2) = \frac{1}{5}(1000) = 200.$$

Also, every tenth integer is divisible by 2 and by 5, so

$$N(a_1a_2) = \frac{1}{10}(1000) = 100.$$

Hence, by the principle of inclusion and exclusion,

$$N(a_1'a_2') = 1000 - 500 - 200 + 100 = 400,$$

which answers (b). Finally, we have

$$N(a_3) = \frac{1}{11}(1000) = 90.9.$$

Of course, since $N(a_3)$ is an integer, this means that

$$N(a_3) = 90.$$

In short,

$$N(a_3) = \lfloor 90.9 \rfloor = 90.$$

Also, every 22nd integer is divisible by 2 and by 11, so

$$N(a_1 a_3) = \left\lfloor \frac{1}{22}(1000) \right\rfloor = \lfloor 45.5 \rfloor = 45.$$

Similarly,

$$N(a_2 a_3) = \left\lfloor \frac{1}{55}(1000) \right\rfloor = \lfloor 18.2 \rfloor = 18.$$

Finally, every 110th integer is divisible by 2, 5, and 11, so

$$N(a_1 a_2 a_3) = \left\lfloor \frac{1}{110}(1000) \right\rfloor = \lfloor 9.1 \rfloor = 9.$$

Thus,

$$N(a_1' a_2' a_3') = 1000 - (500 + 200 + 90) + (100 + 45 + 18) - 9 = 364. \quad \blacksquare$$

Example 7.4 The Number of Integers Relatively Prime to a Given Integer Two integers are *relatively prime* if they have no common divisor greater than 1. Two integers that are not relatively prime must have a common divisor which is a prime. (Why?) Hence, $45 = 3^2 \cdot 5$ and $56 = 2^3 \cdot 7$ are relatively prime. How many integers from 1 to 1000 are relatively prime to 1000? Since $1000 = 2^3 \cdot 5^3$, the only primes dividing 1000 are 2 and 5. So, we want to find the number of integers between 1 and 1000 that are not divisible by 2 or 5. In Example 7.3 we found this to be 400. $\blacksquare$

The method in the previous example generalizes. *Euler's ϕ function* $\phi(n)$ is defined to be the number of integers from 1 to n that are relatively prime to n.

Theorem 7.2 If n is an integer whose unique prime factorization is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

then

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

Proof. An integer from 1 to n is not relatively prime to n if and only if it is divisible by p_1 or p_2 or ... or p_r. Let $A = \{1, 2, \ldots, n\}$ and a_i be the property of being divisible by p_i. Then $N(a_{i_1}a_{i_2}\cdots a_{i_m})$ is obtained by counting elements of A that are multiples of $p_{i_1}p_{i_2}\cdots p_{i_m}$, i.e.,

$$N(a_{i_1}a_{i_2}\cdots a_{i_m}) = \left\lfloor \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_m}} \right\rfloor = \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_m}}$$

since n is divisible by $p_{i_1}p_{i_2}\cdots p_{i_m}$. It follows by the principle of inclusion and exclusion that

$$\phi(n) = N(a_1'a_2'\cdots a_r') = n - n\sum_i \frac{1}{p_i} + n\sum_{i\neq j}\frac{1}{p_ip_j} \mp \cdots + (-1)^r n\frac{1}{p_1p_2\cdots p_r}.$$

The result follows from the observation that

$$(1+x_1)(1+x_2)\cdots(1+x_r) = \sum_{I\subseteq\{1,2,\ldots,r\}}\left(\prod_{i\in I} x_i\right).$$

Q.E.D.

For more on Euler's ϕ function and related results in number theory, see books such as Hardy and Wright [1980]; see also Exercise 32.

Example 7.5 The Woman and the Egg, Fibonacci, and Sieves An old medieval puzzle (Reingold, Nievergelt, and Deo [1977]) goes as follows. An old woman is on her way to the market to sell eggs when she is knocked down by a horseman. Since all the eggs were broken, the horseman offers to pay the damages. The old woman does not remember how many eggs she had. She does remember that when she took them 2 at a time, 1 was left over, and this was also true when she took them 3 or 4 at a time. However, none were left over when she took them 5 at a time. Is there a way to determine the number of eggs the woman had, if it is reasonable to assume that she had at most 25 eggs? A natural way to proceed is to mimic the Sieve of Erastothenes. The Sieve is based on the problem of finding all numbers between 1 and n that are in all of the following sets:

$$\{2k+1 : k \geq 1\}, \{3k+1, 3k+2 : k \geq 1\}, \{5k+1, 5k+2, 5k+3, 5k+4 : k \geq 1\},$$
$$\{7k+1, 7k+2, 7k+3, 7k+4, 7k+5, 7k+6 : k \geq 1\}, \ldots,$$
$$\{pk+1, pk+2, \ldots, pk+p-1 : k \geq 1\},$$

where p is the largest prime less than or equal to n. The old woman's problem can similarly be formulated as the problem of finding all integers between 1 and n in all of the following sets:

$$\{2k+1 : k \geq 1\}, \{3k+1 : k \geq 1\}, \{4k+1 : k \geq 1\}, \{5k : k \geq 1\}.$$

A sieve can be used to solve this problem for $n = 25$ by listing all integers between 1 and 25 and crossing out all numbers of the form $2k$, all numbers of the form $3k$ or $3k+2$, all numbers of the form $4k$ or $4k+2$ or $4k+3$ (the former two types

of numbers would already have been crossed out), and, finally, all numbers of the form $5k+1$, $5k+2$, $5k+3$, or $5k+4$. How many eggs did the woman have? Reingold, Nievergelt, and Deo [1977] show how similar sieve methods can be used to solve more complex problems, such as quickly testing the first 1 million Fibonacci numbers to see which are squares. (The only ones are 1 and 144.) ■

7.1.4 The Probabilistic Case

Suppose that an integer between 1 and 1000 is selected at random. What is the probability that it is not divisible by 2, 5, or 11? The answer is simple. Consider an experiment in which the outcome is one of the integers between 1 and 1000, and the outcomes are equally likely. The number of outcomes signaling the event "is not divisible by 2, 5, or 11" is 364, by the computation in the preceding section. Hence, the probability in question is $364/1000 = .364$.

More generally, suppose we consider an experiment that produces an outcome in a finite set S, the sample space. Let us consider the events $E_1, E_2, \ldots, E_r$. What is the probability that none of these events occur? To answer this, we shall assume, as we have throughout this book, that all outcomes in the sample space S are equally likely. (However, it can be shown that this assumption is not needed to obtain the main result of this subsection.) Let the set A be the set S, and let a_i be the property that an outcome signals event E_i. Let $p_{ijk\ldots}$ be the probability that events E_i and E_j and E_k and ... occur. We conclude from Theorem 7.1 that the probability p that none of the events $E_1, E_2, \ldots, E_r$ occur is given by

$$\begin{aligned} p &= \frac{N(a_1' a_2' \cdots a_r')}{n(S)} \\ &= 1 - \frac{\sum N(a_i)}{n(S)} + \frac{\sum N(a_i a_j)}{n(S)} - \frac{\sum N(a_i a_j a_k)}{n(S)} \pm \cdots + (-1)^r \frac{N(a_1 a_2 \cdots a_r)}{n(S)}, \end{aligned}$$

where $n(S)$ is the number of outcomes in S. Thus,

$$p = 1 - \sum p_i + \sum p_{ij} - \sum p_{ijk} \pm \cdots + (-1)^r p_{12\cdots r}. \tag{7.6}$$

Example 7.6 Antipodal Points Both Covered by Water[3] There is an intriguing problem found in most topology books that asks the reader to prove that on any great circle around the Earth, there exist antipodal points that have the same temperature. A similar type of problem can be asked of a combinatorialist. It is known that ocean covers more than half of the Earth's surface. Show that there are two antipodal points on the Earth that are both covered by water. Let X denote a random point on the Earth. For concreteness, we consider only points of integer latitude and longitude, so the set of all such points is finite. We also let $-X$ denote the point antipodal to X. Consider the following events:

$$\begin{aligned} E_1 &= \text{point } X \text{ is covered by water,} \\ E_2 &= \text{point } -X \text{ is covered by water.} \end{aligned}$$

[3] This example is from Shen [1998].

By (7.6), the probability p that neither event E_1 nor E_2 occurs equals $1-(p_1+p_2)+p_{12}$, where p_i is the probability that event E_i occurs and p_{12} is the probability that both E_1 and E_2 occur. Since p_1 and p_2 are each greater than $1/2$, p_{12} must be positive for p to be between 0 and 1. Thus, there must exist a point X with both properties, i.e., so that X and $-X$ are both covered by water. ■

7.1.5 The Occupancy Problem with Distinguishable Balls and Cells

In Section 2.10, we considered the occupancy problem of placing n distinguishable balls into c distinguishable cells. Let us now ask: What is the probability that no cell will be empty? Let S be the set of distributions of balls to cells, and let E_i be the event that the ith cell is empty. Define A and a_i as above. Then $N(S)=c^n$, $N(a_i)=(c-1)^n$, $N(a_ia_j)=(c-2)^n$, $N(a_ia_ja_k)=(c-3)^n,\ldots$. Moreover, there are $\binom{c}{1}$ ways to choose property a_i, $\binom{c}{2}$ ways to choose properties a_i and a_j, and so on. Hence, the number of distributions of n balls into c cells with no empty cell is given by

$$c^n-\binom{c}{1}(c-1)^n+\binom{c}{2}(c-2)^n-\binom{c}{3}(c-3)^n\pm\cdots+(-1)^c\binom{c}{c}(c-c)^n,$$

which equals

$$\sum_{t=0}^{c}(-1)^t\binom{c}{t}(c-t)^n. \tag{7.7}$$

Then the probability that no cell is empty is given by

$$\frac{c^n-\binom{c}{1}(c-1)^n+\binom{c}{2}(c-2)^n-\binom{c}{3}(c-3)^n+\cdots+(-1)^c\binom{c}{c}(c-c)^n}{c^n},$$

which equals

$$\sum_{t=0}^{c}(-1)^t\binom{c}{t}\left(1-\frac{t}{c}\right)^n, \tag{7.8}$$

since

$$\frac{(c-t)^n}{c^n}=\left(1-\frac{t}{c}\right)^n.$$

Example 7.7 Fast-Food Prizes Suppose that a fast-food outlet gives away three different toys in children's meal packs, one to a package. If we buy six children's meals and each toy is equally likely to be in any one meal pack, what is the probability of getting all three different toys? We imagine placing $n=6$ balls or toys into $c=3$ cells or types of toys. The number of ways the toys can be placed into types so that no cell (or type) is empty is given by Equation (7.7) as

$$3^6-\binom{3}{1}\cdot 2^6+\binom{3}{2}\cdot 1^6-\binom{3}{3}\cdot 0^6=540.$$

The probability of this happening is $540/3^6 = .741$. This can also be computed directly by Equation (7.8) as

$$1 - \binom{3}{1} \cdot \left(\frac{2}{3}\right)^6 + \binom{3}{2} \cdot \left(\frac{1}{3}\right)^6 - \binom{3}{3} \cdot 0^6 = .741.$$

■

7.1.6 Chromatic Polynomials

In Section 3.4 we introduced the idea of a chromatic polynomial of a graph. The principle of inclusion and exclusion can be used to calculate chromatic polynomials. It is interesting to note how the same counting problem can be solved in more than one way. On several occasions in this chapter we shall be able to apply the principle of inclusion and exclusion to count a quantity that we have previously counted in a different way. Consider, for example, the graph of Figure 7.3. We consider all possible colorings of the vertices of G in x or fewer colors. We shall even allow colorings where two vertices joined by an edge get the same color, but we shall call such colorings *improper*, and all others *proper*. Let us consider the set of all colorings, proper or improper, of the graph G in x or fewer colors. There are x^4 such colorings since each of the 4 vertices can be colored by any of the x colors. We shall introduce one property a_i for each edge of the graph G. Thus,

a_1 is the property that a and b get the same color,
a_2 is the property that b and c get the same color,
a_3 is the property that c and d get the same color,
a_4 is the property that d and a get the same color.

To calculate $P(G, x)$, the number of (proper) colorings of G with x or fewer colors, we have to calculate $N(a_1' a_2' a_3' a_4')$. We have $N(a_1) = x^3$, since there are x choices for the color for a and b, then x choices for the color for c, and x for the color for d (recall that improper colorings are allowed). Similarly,

$$N(a_2) = N(a_3) = N(a_4) = x^3.$$

Next,

$$N(a_1 a_2) = x^2.$$

For a and b must receive the same color, and also b and c. Hence, there are x choices for the one color that a, b, and c receive, and then x choices for the color for d. Similar reasoning shows that

$$N(a_1 a_3) = N(a_1 a_4) = N(a_2 a_3) = N(a_2 a_4) = N(a_3 a_4) = x^2.$$

Similarly,

$$N(a_1 a_2 a_3) = N(a_1 a_2 a_4) = N(a_1 a_3 a_4) = N(a_2 a_3 a_4) = x,$$

since in all these cases all the vertices must receive the same color. This reasoning also leads us to conclude

$$N(a_1 a_2 a_3 a_4) = x.$$

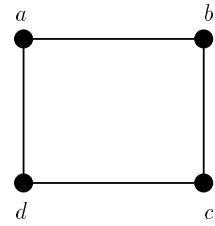


Figure 7.3: A graph.

Hence, by the principle of inclusion and exclusion,

$$\begin{aligned} P(G,x) &= N(a_1'a_2'a_3'a_4') \\ &= x^4 - 4x^3 + 6x^2 - 4x + x \\ &= x^4 - 4x^3 + 6x^2 - 3x. \end{aligned}$$

This computation can be checked by the methods of Chapter 3.

Let us generalize this example as follows. Suppose that G is any graph and we wish to compute $P(G,x)$. Consider the set A of all colorings, proper or improper, of the vertices of G in x or fewer colors. For each edge i, let a_i be the property that the end vertices of edge i get the same color. Suppose that $|V(G)| = n$ and $|E(G)| = r$. Then $N = |A| = x^n$ and

$$P(G,x) = N(a_1'a_2' \cdots a_r').$$

Thus,

$$P(G,x) = x^n - \sum N(a_i) + \sum N(a_ia_j) \mp \cdots + (-1)^e \sum N(a_{i_1}a_{i_2} \cdots a_{i_e}) + \cdots. \quad (7.9)$$

Let us consider the term $N(a_{i_1}a_{i_2} \cdots a_{i_e})$. Suppose that H is the subgraph of G consisting of all the vertices of G and having edges $i_1, i_2, \ldots, i_e$. A subgraph H containing all the vertices of G was called a *spanning subgraph* in Chapter 3. Note that a coloring (proper or improper) of G satisfying properties $a_{i_1}, a_{i_2}, \ldots, a_{i_e}$ is equivalent to a coloring (proper or improper) of H satisfying properties $a_{i_1}, a_{i_2}, \ldots, a_{i_e}$. Now in such a coloring of H, any connected component of H must have all of its vertices colored the same. A color for a component of H can be chosen at random. Thus, the number of colorings of vertices of G in x or fewer colors and satisfying properties $a_{i_1}, a_{i_2}, \ldots, a_{i_e}$ is given by $x^{c(H)}$, where $c(H)$ is the number of connected components of H.

Each spanning subgraph H of e edges and c components corresponds to some set of properties $a_{i_1}, a_{i_2}, \ldots, a_{i_e}$ and will contribute a term $(-1)^e x^c$ to the right-hand side of (7.9). Thus, we have the following theorem.

Theorem 7.3[4] If G is a graph and $h(e,c)$ is the number of spanning subgraphs

[4] This theorem was discovered by Birkhoff [1912] (for graphs arising from maps) and first worked out by inclusion and exclusion by Whitney [1932].

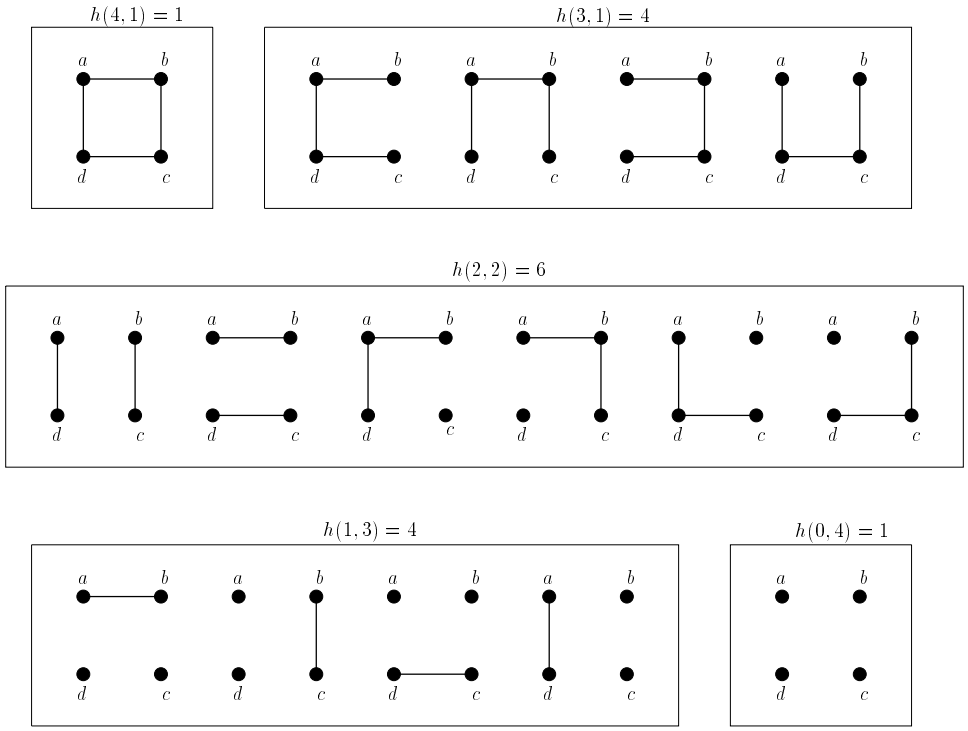


Figure 7.4: The spanning subgraphs of the graph of Figure 7.3.

of e edges and c components, then

$$P(G,x) = \sum_{e,c} (-1)^e h(e,c) x^c.$$

In this theorem, note that $h(0,c)$ is 1 if $c = n$ and 0 otherwise. Note that the theorem gives a quick proof that $P(G,x)$ is a polynomial. In our example of Figure 7.3, we have the following results, which are illustrated in Figure 7.4:

$$h(4,1) = 1, \qquad h(3,1) = 4, \qquad h(2,2) = 6, \qquad h(1,3) = 4, \qquad h(0,4) = 1,$$

and otherwise, $h(e,c) = 0$. Thus, we have

$$\begin{aligned} P(G,x) &= (-1)^4 h(4,1)x + (-1)^3 h(3,1)x + (-1)^2 h(2,2)x^2 + (-1)^1 h(1,3)x^3 \\ &\quad + (-1)^0 h(0,4)x^4 \\ &= x - 4x + 6x^2 - 4x^3 + x^4 \\ &= x^4 - 4x^3 + 6x^2 - 3x, \end{aligned}$$

which agrees with our computation above.

7.1.7 Derangements

The reader will recall from Section 6.1.3 that a derangement is a permutation in which no object is put into its proper position. We shall show how to calculate the number of derangements D_n of a set of n objects by use of the principle of inclusion and exclusion. Consider the set A of all permutations of the n objects. Let a_i be the property that object i is placed in the ith position. Thus,

$$D_n = N(a_1' a_2' \cdots a_n').$$

We have

$$N = n!,$$

the number of permutations. Also,

$$N(a_i) = (n-1)!,$$

for a permutation in which object i returns to its original position is equivalent to a permutation of the remaining objects. Similarly,

$$N(a_i a_j) = (n-2)!$$

and

$$N(a_{i_1} a_{i_2} \cdots a_{i_t}) = (n-t)!.$$

Hence,

$$\sum N(a_{i_1} a_{i_2} \cdots a_{i_t}) = \binom{n}{t}(n-t)!,$$

since there are $\binom{n}{t}$ choices for the properties $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$. It follows by the principle of inclusion and exclusion that

$$\begin{aligned} D_n &= N - \sum N(a_i) + \sum N(a_i a_j) - \sum N(a_i a_j a_k) \pm \cdots + (-1)^n N(a_1 a_2 \cdots a_n) \\ &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! \pm \cdots + (-1)^n \binom{n}{n}(n-n)!. \end{aligned}$$

Simplifying, we have

$$\begin{aligned} D_n &= n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \frac{n!}{3!(n-3)!}(n-3)! \pm \cdots \\ &\quad + (-1)^n \frac{n!}{n!(n-n)!}(n-n)! \\ &= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} \pm \cdots + (-1)^n \frac{1}{n!}\right], \end{aligned}$$

as we have seen previously.

7.1.8 Counting Combinations

In Section 5.3 we studied a variety of counting problems which we solved by means of generating functions. Here we note that the principle of inclusion and exclusion can also be applied to such problems. We illustrate the method by means of an example. Suppose that we are doing a survey and we have three teachers, four plumbers, and six autoworkers whom we are considering interviewing. Suppose that we consider two workers with the same job to be indistinguishable, and we seek the number of ways to choose 11 workers to interview. By the methods of Chapter 5, this can be computed by finding the coefficient of x^{11} in the generating function

$$(1+x+x^2+x^3)(1+x+x^2+x^3+x^4)(1+x+x^2+x^3+x^4+x^5+x^6). \quad (7.10)$$

However, we shall compute it in a different way.

Consider the case where there are infinitely many teachers, plumbers, and autoworkers available, and consider the set A consisting of all the ways of choosing 11 workers to interview. For a particular element of the set A, say it satisfies property a_1 if it uses at least four teachers, property a_2 if it uses at least five plumbers, and property a_3 if it uses at least seven autoworkers. We seek to count all elements of the set A satisfying none of the properties a_i; thus we seek $N(a_1' a_2' a_3')$. To compute this, note that by Theorem 5.4,

$$N = |A| = \binom{3+11-1}{11} = \binom{13}{11} = 78.$$

What is $N(a_1)$? Note that a choice satisfies a_1 if and only if it has at least four teachers. Such a choice is equivalent to choosing seven (arbitrary) workers when there are infinitely many workers of each kind, so can be done, by Theorem 5.4, in

$$\binom{3+7-1}{7} = \binom{9}{7} = 36$$

ways. Thus,

$$N(a_1) = 36.$$

Similarly, a choice satisfying a_2 is equivalent to a choice of six workers when there are infinitely many of each kind, so

$$N(a_2) = \binom{3+6-1}{6} = \binom{8}{6} = 28.$$

Finally,

$$N(a_3) = \binom{3+4-1}{4} = \binom{6}{4} = 15.$$

Next, a choice satisfying both a_1 and a_2 has at least four teachers and at least five plumbers, so is equivalent to a choice of two workers when each is in infinite supply. Thus,

$$N(a_1 a_2) = \binom{3+2-1}{2} = \binom{4}{2} = 6.$$

Similarly, a choice satisfying a_1 and a_3 is equivalent to a choice of no workers when each is in infinite supply; as there is exactly one way to choose no workers,

$$N(a_1a_3) = 1.$$

Also, there is no way to choose 11 workers, at least 5 of whom are plumbers and at least 7 of whom are autoworkers, so

$$N(a_2a_3) = 0.$$

Similarly,

$$N(a_1a_2a_3) = 0.$$

Thus, by the principle of inclusion and exclusion, the desired number of choices is

$$78 - (36 + 28 + 15) + (6 + 1 + 0) - 0 = 6.$$

It is easy to check this result by computing the coefficient of x^{11} in the generating function (7.10).

7.1.9 Rook Polynomials[5]

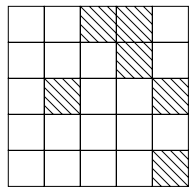
In Examples 5.10, 5.14, and 6.15, we studied the notion of rook polynomial of a board B consisting of acceptable (darkened) or unacceptable squares. If as in Figures 5.1 and 5.2, the board in B has a predominance of darkened squares, it is useful to consider the *complementary board* B' of B, the board obtained from B by interchanging acceptable and forbidden squares. Suppose that B is an $n \times m$ board and we are interested in $r_n(B)$, the number of ways to place n nontaking rooks on acceptable squares of the board B. We shall show that we can obtain $r_n(B)$ from $R(x, B')$, the rook polynomial of the complementary board, rather than from $R(x, B)$. The former rook polynomial, based on a board with fewer darkened squares, will be easier to compute. We may assume that $n \leq m$. For if $n > m$, then $r_n(B) = 0$. Note that we shall not be computing $r_j(B)$ for $j < n$, only for the special case $j = n$. In Exercise 37 of Section 7.2 the reader is asked to generalize the results to arbitrary $r_j(B)$, $j \leq n$.

Let us say that an *assignment* of n nontaking rooks to an $n \times m$ board B means that each rook is placed in a square, acceptable or not, with no two rooks in the same row and no two rooks in the same column. There are

$$P(m, n) = m(m-1)\cdots(m-n+1)$$

possible assignments. For we choose one of m positions in the first row, then one of $m-1$ positions in the second row, ..., and, finally, one of $m-n+1$ positions in the nth row. Let A be the set of all possible assignments for board B, and let a_i be the property that an assignment has a rook in a forbidden square in the ith column. Then $r_n(B)$ is given by the number of assignments having none of the

[5]This subsection may be omitted.



B'

Figure 7.5: The complementary board B' of the board B of Figure 5.1.

properties $a_1, a_2, \ldots, a_m$. We compute this number using the principle of inclusion and exclusion.

Given t, we shall see how to compute

$$\sum N(a_{i_1} a_{i_2} \cdots a_{i_t}),$$

where t must, of course, be at most m. Note that this sum is 0 if $t > n$ because there could be no assignment with rooks in t different columns, let alone in a forbidden square in t different columns. If $t \leq n$, consider the complementary board B'. An assignment of n nontaking rooks to B with a rook in forbidden position in each of t columns of B corresponds to an assignment of t nontaking rooks to acceptable squares of the board B'—this can be done in $r_t(B')$ ways—and then an arbitrary placement of the remaining $n-t$ rooks in any of the remaining $m-t$ columns—this can be done in $P(m-t, n-t)$ ways. Thus, for $t \leq n$,

$$\sum N(a_{i_1} a_{i_2} \cdots a_{i_t}) = P(m-t, n-t) r_t(B').$$

By the principle of inclusion and exclusion, we conclude that

$$\begin{aligned} r_n(B) = {} & P(m,n) - P(m-1, n-1) r_1(B') \pm \cdots + \\ & (-1)^t P(m-t, n-t) r_t(B') \pm \cdots + (-1)^n P(m-n, 0) r_n(B'). \end{aligned} \tag{7.11}$$

Let us apply this result to the 5×5 board B of Figure 5.1 and compute $r_5(B)$. The complementary board B' is shown in Figure 7.5. By the reduction results of Exercise 17, Section 5.1, and Example 5.14, one can show that

$$R(x, B') = 1 + 6x + 11x^2 + 6x^3 + x^4. \tag{7.12}$$

Using (7.12), noting that $P(a,a) = a!$, and applying (7.11), we have

$$r_5(B) = 5! - 4!(6) + 3!(11) - 2!(6) + 1!(1) - 0!(0) = 31.$$

EXERCISES FOR SECTION 7.1

1. Three premium cable television channels, A, B, and C, are available in a city. The following results were obtained in a survey of the households of the city: 20 percent

subscribed to A, 16 percent to B, 14 percent to C, 8 percent to both A and B, 5 percent to both A and C, 4 percent to both B and C, and 2 percent to all three. What percentage of the households subscribed to none of the channels?

2. In an experiment, there are two kinds of treatments, the controls and the noncontrols. There are 3 controls and 80 experimental units or blocks. Each control is used in 25 blocks, each pair of controls is used in the same block 11 times, and all three controls are used in the same block together 12 times. In how many blocks are none of the controls used? (We shall study similar conditions on experimental designs in detail in Chapter 9.)

3. A cigarette company surveys 200,000 people. Of these, 130,000 are males, according to the company's report. Also, 90,000 are smokers and 10,000 of those surveyed have cancer. However, of those surveyed, there are 7000 males with cancer, 8000 smokers with cancer, and 5000 male smokers. Finally, there are 1000 male smokers with cancer. How many female nonsmokers without cancer are there? Is there something wrong with the cigarette company's report?

4. Eight hundred people were tested for immunity to the diseases tuberculosis, rubella, and smallpox. Of the 800 people, 350 were found to have immunity to tuberculosis, 450 to rubella, 450 to smallpox, 150 to tuberculosis and rubella, 200 to rubella and smallpox, 250 to tuberculosis and smallpox, and 100 to tuberculosis, rubella, but not smallpox. How many people were found to have immunity to none of the diseases?

5. (a) Suppose that among 1000 households surveyed, 30 have neither an exercise bicycle nor a treadmill, 50 have only an exercise bicycle, and 60 have only a treadmill. How many households have both?

   (b) How many arrangements of the digits $0, 1, 2, \ldots, 9$ are there in which the first digit is greater than 2 and the last digit is less than 7?

   (c) How many DNA sequences of length 10 are there with at least one of each base A, G, C, T?

6. Find an expression for the number of objects in a set A which have at least one of the properties a_1, a_2, $\ldots$, a_r.

7. One hundred twenty water samples were tested for traces of three different types of chemicals: mercury, arsenic, and lead. Of the 120 samples, 17 were found to have mercury, 15 to have arsenic, 14 to have lead, 10 to have mercury and arsenic, 7 to have arsenic and lead, 15 to have mercury and lead, and 5 to have mercury, arsenic, but no lead. How many samples had a trace of at least one of the three chemicals?

8. Of 100 cars tested at an inspection station, 9 had defective headlights; 8 defective brakes; 7 defective horns; 2 defective windshield wipers; 4 defective headlights and brakes; 3 defective headlights and horns; 2 defective headlights and windshield wipers; 3 defective brakes and horns; none defective brakes and windshield wipers; 1 defective horn and windshield wipers; 1 defective headlights, brakes and horn; 1 defective headlights, horn, and windshield wipers; and none had any other combination of defects. Find the number of cars that had at least one of the defects in question.

9. A total of 100 students at a college were interviewed. Of these, 38 were taking a French course; 45 were taking a physics course; 28 a mathematics course; 25 a history course; 22 were taking French and physics; 23 French and mathematics; 10 physics and mathematics; 1 French and history; 21 physics and history; 14 mathematics

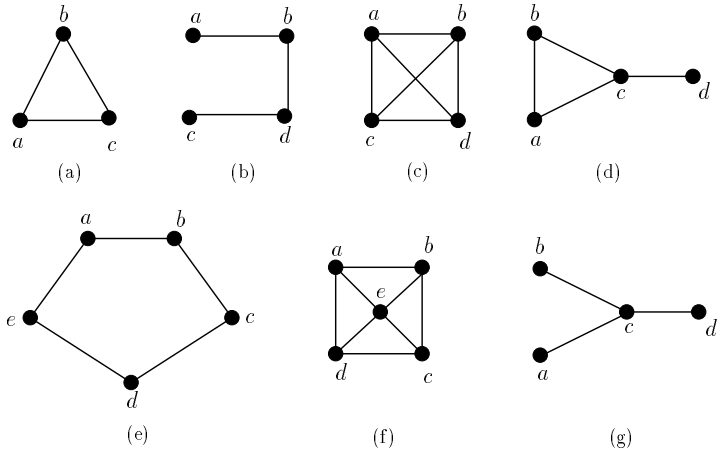


Figure 7.6: Graphs for exercises of Section 7.1.

and history; 11 French, physics, and mathematics; 8 French, physics, and history; 6 French, mathematics, and history; 6 physics, mathematics, and history; and 5 were taking courses in all four subjects. How many students were taking at least one course in the subjects in question?

10. A troubleshooter has pinpointed three 3 files as the source of potential problems on a computer. He has used each file in a test 12 times, each pair of files in the same test together 6 times, and all 3 files in the same test together 4 times. In 8 tests, none of the files were used. How many tests were performed altogether?
11. How many integers between 1 and 10,000 inclusive are divisible by none of 5, 7, and 11?
12. How many integers between 1 and 600 inclusive are divisible by none of 2, 3, and 5?
13. How many integers between 1 and 600 inclusive are divisible by none of 2, 3, 5, and 7?
14. Nine accidents occur during a week. Write an expression for computing the probability that there is at least one accident each day.
15. A total of six misprints occur on five pages of a book. What is the probability that each of these pages has at least one misprint?
16. Twenty light particles hit a section of the retina that has nine cells. What is the probability that at least one cell is not hit by a light particle?
17. How many permutations of $\{1, 2, 3, 4, 5, 6\}$ have the property that $i + 1$ never immediately follows i?
18. Use the principle of inclusion and exclusion (not Theorem 7.3) to find the chromatic polynomial of each of the graphs of Figure 7.6.
19. Use Theorem 7.3 to find the chromatic polynomial of each of the graphs of Figure 7.6.
20. The *star* $S(1, n)$ is the graph consisting of one central vertex and n neighboring vertices, with no other edges. Figure 7.7 shows some stars. Find the chromatic polynomial of $S(1, n)$ using the methods of Section 7.1.6.

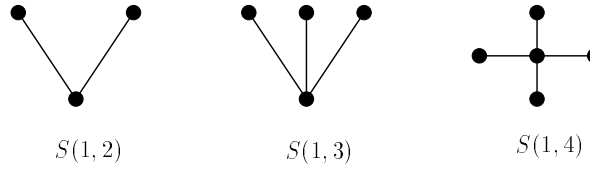


Figure 7.7: Some stars.

21. Use the principle of inclusion and exclusion to count the number of ways to choose:

    (a) 8 elements from a set of 4 a's, 4 b's, and 5 c's

    (b) 9 elements from a set of 3 a's, 4 b's, and 5 c's

    (c) 12 elements from a set of 6 a's, 6 b's, and 4 c's

22. Verify Equation (7.12).

23. Use Equation (7.11) to compute $r_n(B)$ if B is the $n \times n$ board with all squares acceptable.

24. Use Equation (7.11) and earlier reduction results to compute $r_5(B)$ for board B of Figure 5.2.

25. Suppose that $r = 3$ and that an object has exactly two properties. How many times is the object counted in computing:

    (a) $\sum N(a_i)$? (b) $\sum N(a_i a_j)$?

26. Suppose that $r = 8$ and that an object has exactly three properties. How many times is the object counted in computing:

    (a) $\sum N(a_i)$? (b) $\sum N(a_i a_j)$? (c) $\sum N(a_i a_j a_k)$? (d) $\sum N(a_i a_j a_k a_l)$?

27. Suppose that d distinguishable CDs are placed in n distinguishable CD players. More than one CD can go in a player. We distinguish placing CD_5 in player 1 from placing CD_5 in player 2, and also distinguish placing CD_5 in player 1 from placing CD_6 in player 1, and so on. Suppose that the CDs are distributed so that no players are empty. In how many ways can this be done?

28. Use inclusion and exclusion to find the number of solutions to the equation

$$x_1 + x_2 + x_3 = 15$$

    in which each x_i is a nonnegative integer and $x_i \leq 7$.

29. Use inclusion and exclusion to find the number of solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 18$$

    in which each x_i is a positive integer and $x_i \leq 8$.

30. Find the number of n-digit codewords from the alphabet $\{0, 1, 2, \ldots, 9\}$ in which the digits 1, 2, and 3 each appear at least once.

31. (a) Find the number of onto functions from a set with five elements to a set with three elements.

(b) If m and n are positive integers, find a formula for the number of onto functions from a set with m elements to a set with n elements.

32. Recall that every positive integer n can be written in a unique way as the product of powers of primes,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_i \geq 1$, all i. The *Moebius function* $\mu(n)$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } e_i > 1, \text{ any } i \\ (-1)^r & \text{if } e_1, e_2, \ldots, e_r \text{ all equal 1.} \end{cases}$$

Thus, $\mu(100) = 0$ since 2^2 is a factor of 100, and $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$.

(a) Show from the principle of inclusion and exclusion that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1, \end{cases} \tag{7.13}$$

where the sum in (7.13) is taken over all integers d that divide n. For example,

$$\begin{aligned} \sum_{d|12} \mu(d) &= \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) \\ &= 1 + (-1) + (-1) + 0 + (-1)^2 + 0 \\ &= 0. \end{aligned}$$

(b) Suppose that f and g are functions such that

$$f(n) = \sum_{d|n} g(d).$$

Show from the result in part (a) that

$$g(n) = \sum_{d|n} f\left(\frac{n}{d}\right) \mu(d). \tag{7.14}$$

Equation (7.14) is called the *Moebius inversion formula*. For generalizations of this formula of significance in combinatorics, see Rota [1964] (see also Berge [1971], Hall [1986], and Liu [1972]).

(c) Show that if $\phi(n)$ is the Euler ϕ function, then

$$n = \sum_{d|n} \phi(d).$$

(d) Conclude that

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

(e) Show that

$$\phi(p^c) = p^c \left(1 - \frac{1}{p}\right).$$

33. (Cohen [1978]) Each of n gentlemen checks both a hat and an umbrella. The hats are returned at random and then the umbrellas are returned at random independently. What is the probability that no man gets back both his hat and his umbrella?

34. Exercises 34 and 35 consider permutations with restrictions on certain patterns. To say that the *pattern uv does not appear* in a permutation $j_1 j_2 j_3 \cdots j_n$ of $\{1, 2, \ldots, n\}$ means that $j_i j_{i+1}$ is never uv. Similarly, to say that the *pattern uvw does not appear* means that $j_i j_{i+1} j_{i+2}$ is never uvw. Let b_n be the number of permutations of the set $\{1, 2, \ldots, n\}$ in which the patterns $12, 23, \ldots, (n-1)n$ do not appear. Find b_n.

35. Find the number of permutations of $\{1, 2, 3, 4, 5, 6\}$ in which neither the pattern 125 nor the pattern 34 appears (see Exercise 34).

36. Find the number of ways in which the letters a, a, b, b, c, c, c, d, d can be arranged so that two letters of the same kind never appear consecutively.

37. How many codewords of length 9 from the alphabet $\{0, 1, 2\}$ have three of each digit, but no three consecutive digits the same?

38. How many RNA chains have two A's, two U's, two C's, and two G's, and have no repeated base?

39. In our study of partitions of an integer (Exercises 12–16, Section 5.3), let $p^*(k)$ be the number of partitions of k with distinct integers and $p_0(k)$ be the number of partitions of k with odd integers.

    (a) Define a set A and properties a_i and b_i for elements of A so that

    $$p_0(k) = N(a_1' a_2' \cdots)$$

    and

    $$p^*(k) = N(b_1' b_2' \cdots).$$

    (b) Show that A, a_i, and b_i in part (a) can be chosen so that

    $$N(a_{i_1} a_{i_2} \cdots a_{i_k}) = N(b_{i_1} b_{i_2} \cdots b_{i_k})$$

    for all k. Conclude that $p_0(k) = p^*(k)$. (This result was derived by generating functions in Exercise 15, Section 5.3.)

40. (Shen [1998]) A sphere is colored in two colors: 10 percent of its surface is white, the remaining part is black. Prove that there is a cube inscribed in the sphere such that all its 8 vertices are black. (*Hint:* Consider Example 7.6.)

7.2 THE NUMBER OF OBJECTS HAVING EXACTLY m PROPERTIES

7.2.1 The Main Result and Its Applications

Let us return to the general situation of a set of N objects, each of which may or may not have each of r different properties, a_1, a_2, ..., a_r. There are situations where we want to know how many objects have exactly m of these properties. Let

e_m be the number of objects having exactly m properties, $m \leq r$. To express a formula for e_m, suppose that for $t \geq 1$, we let

$$s_t = \sum N(a_{i_1} a_{i_2} \cdots a_{i_t}),$$

where the sum is taken over all choices of t distinct properties a_{i_1}, a_{i_2}, ..., a_{i_t}. Then we have the following theorem.

Theorem 7.4 The number of objects having exactly m properties if there are r properties and $m \leq r$ is given by

$$\begin{aligned} e_m = s_m - \binom{m+1}{1} s_{m+1} + \binom{m+2}{2} s_{m+2} - \binom{m+3}{3} s_{m+3} \pm \cdots \\ + (-1)^p \binom{m+p}{p} s_{m+p} \pm \cdots + (-1)^{r-m} \binom{m+r-m}{r-m} s_r. \end{aligned} \tag{7.15}$$

The reader should note that if s_0 is taken to be N, Theorem 7.4 yields the principle of inclusion and exclusion as a special case when $m = 0$.

We prove this theorem in Section 7.2.2. Here, let us apply it to several examples. In particular, let us return to Example 7.2. How many cars exceed the environmental standards on exactly one pollutant? We seek e_1. To compute e_1, we note that by the computation in the example,

$$\begin{aligned} s_1 &= 6 + 4 + 3 = 13, \\ s_2 &= 3 + 2 + 1 = 6, \\ s_3 &= 1. \end{aligned}$$

Thus, by Theorem 7.4,

$$\begin{aligned} e_1 &= s_1 - \binom{2}{1} s_2 + \binom{3}{2} s_3 \\ &= 13 - 2(6) + 3(1) \\ &= 4. \end{aligned}$$

Example 7.8 The Hatcheck Problem (Example 6.9 Revisited) In Example 6.9, we considered a situation in which the hats of n gentlemen are returned at random. In this situation, let us compute the number of ways in which exactly one gentleman gets his hat back. Let us consider the set A of possible ways of returning hats to gentlemen if they are returned at random—these correspond to permutations—and let a_i be the property that the ith gentleman gets his own hat back. In Section 7.1.7, in dealing with derangements, we calculated

$$\begin{aligned} N(a_i) &= (n-1)!, \quad \text{all } i, \\ N(a_i a_j) &= (n-2)!, \quad \text{all } i \neq j, \end{aligned}$$

and in general

$$N(a_{i_1} a_{i_2} \cdots a_{i_t}) = (n-t)!.$$

Hence,

$$s_t = \binom{n}{t}(n-t)!$$

since there are $\binom{n}{t}$ ways to pick the t properties $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$. Then by Theorem 7.4, with $r = n$ and $m = 1$, we have

$$\begin{aligned}
e_1 = \; & s_1 - \binom{2}{1}s_2 + \binom{3}{2}s_3 - \binom{4}{3}s_4 \pm \cdots + (-1)^{n-1}\binom{n}{n-1}s_n \\
= \; & \binom{n}{1}(n-1)! - \binom{2}{1}\binom{n}{2}(n-2)! + \binom{3}{2}\binom{n}{3}(n-3)! - \binom{4}{3}\binom{n}{4}(n-4)! \\
& \pm \cdots + (-1)^{n-1}\binom{n}{n-1}\binom{n}{n}(n-n)! \\
= \; & \frac{n!}{1!(n-1)!}(n-1)! - \frac{2!}{1!1!}\frac{n!}{2!(n-2)!}(n-2)! + \frac{3!}{2!1!}\frac{n!}{3!(n-3)!}(n-3)! \\
& - \frac{4!}{3!1!}\frac{n!}{4!(n-4)!}(n-4)! \pm \cdots + (-1)^{n-1}\frac{n!}{(n-1)!1!} \\
= \; & n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} \pm \cdots + (-1)^{n-1}\frac{n!}{(n-1)!} \\
= \; & n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} \pm \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right] \\
= \; & nD_{n-1}.
\end{aligned}$$

This result is clear, for we pick one gentleman to get his hat back—this can be done in n ways—and then choose a derangement of the rest of the gentlemen—this can be done in D_{n-1} ways.

We conclude that the probability that exactly one gentleman gets his hat back is

$$\frac{nD_{n-1}}{n!} = \frac{D_{n-1}}{(n-1)!},$$

which approaches $1/e$ as n approaches infinity, since $D_n/n!$ does. Thus, in the long run, the probability that exactly one gentleman gets his hat back is the same as the probability that no gentlemen get their hats back. ■

Example 7.9 Testing Psychic Powers In some psychic experiments, we present a sequence of n elements in an order unknown to a person who claims to have psychic powers. That person predicts the order in advance. We count the number of correct elements, that is, the number of elements whose place in the sequence is predicted exactly right. Suppose that in a sequence of 10 elements, a person gets five right. Would we take this as evidence of psychic powers? To answer the question, we ask whether the observed number of successes is very unlikely if the person is only guessing. In particular, we ask what is the probability of guessing at least five elements correctly. (We are really interested in how likely it is the person did at least as well as he did.) The number of ways to guess exactly m elements correctly in a sequence of n elements can be computed from Theorem 7.4. We let A be the

set of all permutations of the set $\{1, 2, \ldots, n\}$ and a_i be the property that i is in the ith position. Then $N(a_i)$, $N(a_i a_j)$, and so on, are exactly as in our analysis of the hatcheck problem, and so is s_t for every t. Thus, one can show that the probability of guessing exactly m positions correctly is given by

$$P_m^n = \frac{1}{m!}\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} \pm \cdots + (-1)^{(n-m)}\frac{1}{(n-m)!}\right]. \tag{7.16}$$

The detailed verification of (7.16) is left as an exercise (Exercise 26). The probability of guessing at least five positions right out of a sequence of 10 is given by

$$\begin{aligned} P_5^{10}+P_6^{10}+P_7^{10}+P_8^{10}+P_9^{10}+P_{10}^{10} &= .00306+.00052+.00007+.00001+.00000+.00000 \\ &= .00366. \end{aligned}$$

(Notice that the next-to-last .00000 here is in fact exactly 0, while the last is actually 1/10!.) We conclude that the probability of achieving this much success by guessing is *very* small. We would have some evidence to conclude that the person *does* seem to have psychic powers. For further references on tests of psychic powers and other applications of the notion of derangement of interest to psychologists, see Barton [1958], Utts [1991], and Vernon [1936]. ■

Example 7.10 RNA Chains Let us find the number of RNA chains of length n with exactly two U's. We can calculate this number directly. For to get an RNA chain of length n with exactly two U's, we choose two positions out of n for the U's and then have three choices of base for each of the remaining $n-2$ positions. This gives us

$$\binom{n}{2}3^{n-2}$$

chains. It is interesting to see how we can obtain this number from Theorem 7.4. Let A be the set of all n-digit sequences from the alphabet U, A, C, G, and let a_i be the property that there is a U in the ith position. Then we seek e_2. Note that

$$N(a_{i_1}a_{i_2}\cdots a_{i_t}) = 4^{n-t},$$

for we have four choices for the ith element in the chain if $i \neq i_1, i_2, \ldots, i_t$. Hence,

$$s_t = \binom{n}{t}4^{n-t},$$

since there are t properties to choose from n properties. We conclude by Theorem 7.4 that

$$\begin{aligned} e_2 &= s_2 - \binom{3}{1}s_3 + \binom{4}{2}s_4 \mp \cdots + (-1)^p\binom{p+2}{p}s_{p+2} \pm \cdots + (-1)^{n-2}\binom{n}{n-2}s_n \\ &= \binom{n}{2}4^{n-2} - \binom{3}{1}\binom{n}{3}4^{n-3} + \binom{4}{2}\binom{n}{4}4^{n-4} \mp \cdots \\ &\quad + (-1)^p\binom{p+2}{p}\binom{n}{p+2}4^{n-p-2} \pm \cdots + (-1)^{n-2}\binom{n}{n-2}\binom{n}{n}4^{n-n}. \end{aligned}$$

To evaluate this expression for e_2, note that

$$\begin{aligned}(-1)^p \binom{p+2}{p}\binom{n}{p+2}4^{n-p-2} &= (-1)^p \frac{(p+2)!}{p!2!}\frac{n!}{(p+2)!(n-p-2)!}4^{n-p-2} \\ &= (-1)^p \frac{n(n-1)}{2}\frac{(n-2)!}{p!(n-p-2)!}4^{n-p-2} \\ &= \binom{n}{2}(-1)^p\binom{n-2}{p}4^{n-p-2}.\end{aligned}$$

Thus

$$e_2 = \binom{n}{2}\sum_{p=0}^{n-2}\binom{n-2}{p}(-1)^p 4^{n-p-2}.$$

By the binomial expansion (Theorem 2.7),

$$e_2 = \binom{n}{2}(4-1)^{n-2} = \binom{n}{2}3^{n-2}.$$

This result agrees with our initial computation. In this case, use of Theorem 7.4 was considerably more difficult! ■

Example 7.11 Legitimate Codewords (Example 6.4 Revisited) In Example 6.4 we defined a codeword from the alphabet $\{0,1,2,3\}$ as *legitimate* if it had an even number of 0's and we let a_k be the number of legitimate codewords of length k. In Section 6.3.1 we used generating functions to show that

$$a_k = \frac{1}{2}(2)^k + \frac{1}{2}(4)^k.$$

Here, we shall derive the same result using Theorem 7.4. Let A be the set of all sequences of length k from $\{0,1,2,3\}$, and let a_i be the property that the ith digit is 0, $i = 1,2,\ldots,k = r$. We seek the number of elements of A having an even number of these properties; that is, we seek $e_0 + e_2 + e_4 + \cdots$. To compute this sum, note that

$$s_t = \binom{k}{t}4^{k-t}$$

for

$$N(a_{i_1}a_{i_2}\cdots a_{i_t}) = 4^{k-t}.$$

From this and Theorem 7.4, one can show by algebraic manipulation that

$$e_0 + e_2 + e_4 + \cdots = \frac{1}{2}(2)^k + \frac{1}{2}(4)^k. \tag{7.17}$$

An easier way to show (7.17) is to use the following theorem, whose proof comes in Section 7.2.2. ■

Theorem 7.5 If there are r properties, the number of objects having an even number of the properties is given by

$$e_0 + e_2 + e_4 + \cdots = \frac{1}{2}\left[s_0 + \sum_{t=0}^{r}(-2)^t s_t\right]$$

and the number of objects having an odd number of the properties is given by

$$e_1 + e_3 + e_5 + \cdots = \frac{1}{2}\left[s_0 - \sum_{t=0}^{r}(-2)^t s_t\right].$$

Applying Theorem 7.5 to Example 7.11, and recalling that s_0 is taken to be N, we find using the binomial expansion (Theorem 2.7) that

$$\begin{aligned} e_0 + e_2 + e_4 + \cdots &= \frac{1}{2}\left[4^k + \sum_{t=0}^{k}(-2)^t \binom{k}{t} 4^{k-t}\right] \\ &= \frac{1}{2}\left[4^k + (-2+4)^k\right] \\ &= \frac{1}{2}\left[4^k + 2^k\right], \end{aligned}$$

which agrees with (7.17).

Example 7.12 Cosmic Rays and Occupancy Problems Suppose that we have a Geiger counter with c cells which is exposed to a shower of cosmic rays, getting hit by n rays. What is the probability that exactly q counters will go off? To answer this question, we can follow the analysis in Section 7.1.4, where we introduced a sample space S and events E_i. Here, S consists of all distributions of n rays to c cells, and E_i is the event that counter i is not hit. We want the probability that exactly $m = c - q$ counters are not hit, that is, that exactly m of the events in question occur. We can introduce a set A and properties a_i exactly as in Section 7.1.4, and observe that among events $E_1, E_2, \ldots, E_r$, the probability that exactly m of them will occur can be computed from Theorem 7.4 by using $e_m/N(S)$. In our example, we can compute e_m by thinking of this as an occupancy problem and using the computations for $N(a_i)$, $N(a_i a_j)$, and so on, from Section 7.1.5. Then we find that

$$s_t = \sum N(a_{i_1} a_{i_2} \cdots a_{i_t}) = \binom{c}{t}(c-t)^n.$$

Thus, one can show from Theorem 7.4 that the probability that exactly m of the events $E_1, E_2, \ldots, E_r$ will occur is given by

$$\binom{c}{m}\sum_{p=0}^{c-m}(-1)^p \binom{c-m}{p}\left(1 - \frac{m+p}{c}\right)^n. \tag{7.18}$$

A detailed verification is left to the reader (Exercise 28). The result in (7.18) can also be derived directly from the case $m = 0$ (see Exercise 29). ■

For a variety of other applications of Theorem 7.4, see Feller [1968], Irwin [1955], or Parzen [1992].

7.2.2 Proofs of Theorems 7.4 and 7.5[6]

We close this section by presenting proofs of Theorems 7.4 and 7.5.

Proof of Theorem 7.4. The proof is similar to the proof of Theorem 7.1. As a preliminary, we note that

$$\begin{aligned}\binom{m+j}{m+p}\binom{m+p}{p} &= \frac{(m+j)!}{(m+p)!(j-p)!}\frac{(m+p)!}{p!m!} \\ &= \frac{(m+j)!}{m!p!(j-p)!} \\ &= \frac{(m+j)!}{m!j!}\frac{j!}{p!(j-p)!} \\ &= \binom{m+j}{m}\binom{j}{p}.\end{aligned}$$

Thus,

$$\binom{m+j}{m+p}\binom{m+p}{p} = \binom{m+j}{m}\binom{j}{p}. \tag{7.19}$$

Let us now consider Equation (7.15). If an object has fewer than m properties a_i, it is not counted in calculating e_m and it is not counted in any of the terms in the right-hand side of (7.15). Suppose that an object has exactly m of the properties. It is counted exactly once in calculating e_m, and counted exactly once in calculating the right-hand side of (7.15), namely in calculating s_m. Finally, suppose that an object has more than m properties, say $m+j$ properties. It is not counted in calculating e_m. We shall argue that the number of times it is counted in the right-hand side of (7.15) is 0. The object is counted $\binom{m+j}{m}$ times in calculating s_m: It is counted once for every m properties we can choose out of the $m+j$ properties the object has. It is counted $\binom{m+j}{m+1}$ times in calculating s_{m+1}. In general, it is counted $\binom{m+j}{m+p}$ times in calculating s_{m+p} for $p \le j$. It is not counted otherwise. Hence, the total number of times the object is counted in the right-hand side of (7.15) is calculated by multiplying $\binom{m+j}{m+p}$ by $(-1)^p\binom{m+p}{p}$, the coefficient of s_{m+p}, and adding these terms for $p=0$ up to j. We obtain

$$\begin{aligned}&\binom{m+j}{m} - \binom{m+j}{m+1}\binom{m+1}{1} + \binom{m+j}{m+2}\binom{m+2}{2} \mp \cdots \\ &+ (-1)^p\binom{m+j}{m+p}\binom{m+p}{p} \pm \cdots + (-1)^j\binom{m+j}{m+j}\binom{m+j}{j}.\end{aligned} \tag{7.20}$$

Now by (7.19), (7.20) becomes

$$\binom{m+j}{m} - \binom{m+j}{m}\binom{j}{1} + \binom{m+j}{m}\binom{j}{2} \mp \cdots + (-1)^j\binom{m+j}{m}\binom{j}{j},$$

[6] This subsection may be omitted.

which equals

$$\binom{m+j}{m}\left[\binom{j}{0}-\binom{j}{1}+\binom{j}{2}\mp\cdots+(-1)^j\binom{j}{j}\right]. \tag{7.21}$$

By Theorem 2.9, the bracketed material in (7.21) equals 0 [it arises by expanding $(1-1)^j$ using the binomial expansion], so (7.21) is 0. This completes the proof of Theorem 7.4. Q.E.D.

Proof of Theorem 7.5. Let $E(x)=\sum e_m x^m$ be the ordinary generating function for the sequence $e_0, e_1, e_2, \ldots$. By Theorem 7.4,

$$\begin{aligned}
E(x) &= [s_0 - s_1 + s_2 - \cdots + (-1)^r s_r] \\
&\quad + \left[s_1 - \binom{2}{1}s_2 + \binom{3}{2}s_3 - \cdots + (-1)^{r-1}\binom{r}{r-1}s_r\right] x \\
&\quad + \left[s_2 - \binom{3}{1}s_3 + \binom{4}{2}s_4 - \cdots + (-1)^{r-2}\binom{r}{r-2}s_r\right] x^2 \\
&\quad + \cdots \\
&\quad + \left[s_m - \binom{m+1}{1}s_{m+1} + \binom{m+2}{2}s_{m+2} - \cdots + (-1)^{r-m}\binom{m+r-m}{r-m}s_r\right] x^m \\
&\quad + \cdots \\
&\quad + s_r x^r \\
&= s_0 \\
&\quad + s_1[x-1] \\
&\quad + s_2\left[x^2 - \binom{2}{1}x + 1\right] \\
&\quad + s_3\left[x^3 - \binom{3}{1}x^2 + \binom{3}{2}x - 1\right] \\
&\quad + \cdots \\
&\quad + s_m\left[x^m - \binom{m}{1}x^{m-1} + \binom{m}{2}x^{m-2} + \cdots + (-1)^{m-1}\binom{m}{m-1}x + (-1)^m\right] \\
&\quad + \cdots \\
&\quad + s_r\left[x^r - \binom{r}{1}x^{r-1} + \binom{r}{2}x^{r-2} + \cdots + (-1)^{r-1}\binom{r}{r-1}x + (-1)^r\right].
\end{aligned}$$

Thus,

$$E(x) = \sum_{m=0}^{r} s_m (x-1)^m. \tag{7.22}$$

The first part of the theorem follows by noting that

$$e_0 + e_2 + e_4 + \cdots = \frac{1}{2}\left[E(1) + E(-1)\right]$$

and taking $x = 1$ and $x = -1$ in (7.22). The second part of the theorem follows by noting that

$$e_1 + e_3 + e_5 + \cdots = \frac{1}{2}\left[E(1) - E(-1)\right]. \qquad \text{Q.E.D.}$$

EXERCISES FOR SECTION 7.2

1. In Exercise 1, Section 7.1, what percentage of the households subscribe to exactly one of the channels?
2. In Exercise 2, Section 7.1, how many blocks use exactly two controls?
3. In Exercise 4, Section 7.1, how many people were immune to exactly one of the diseases?
4. In Exercise 8, Section 7.1, find the number of cars having exactly two of the defects in question.
5. In Exercise 9, Section 7.1, find the number of students taking exactly three of the subjects in question.
6. How many words of length 6 have an even number of vowels?
7. A variant of Montmort's "probleme des rencontres" discussed in Section 6.1.3 is the following. A deck of n cards is laid out in a row on the table. Cards of a second deck with n cards are placed one by one at random on top of the first set of cards. You get m points if there are m matches between the first and second decks.
   (a) How many ways are there to get 2 points if $n = 4$?
   (b) What is the probability of getting 7 points if $n = 9$?
8. The names on the files of 10 different job candidates appearing for an interview were unfortunately lost, and a new receptionist placed the names on the files at random. In how many ways could this be done so that exactly 3 candidates' files were labeled properly?
9. In the hatcheck problem, use our formula for e_1 to determine the probability that exactly one gentleman gets his hat back if there are 3 gentlemen.
10. In the hatcheck problem, if there are 4 gentlemen, compute the number of ways that exactly 2 of them will get their hats back.
11. Compute e_m for the hatcheck problem for arbitrary m.
12. (a) If four fair coins are tossed, use Theorem 7.4 to compute the probability that there will be exactly 2 heads.

(b) Check your answer by computing it directly.

13. Use Theorem 7.4 to compute the number of ways to get exactly m heads if a coin is tossed n times.

14. (a) Use Theorem 7.4 to find the number of permutations of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ in which exactly 4 integers are in their natural positions.

    (b) Check your answer by computing it directly.

15. (a) Use Theorem 7.4 to compute the number of legitimate codewords of length 7 from the alphabet $\{0, 1, 2\}$ if a codeword is legitimate if and only if it has exactly three 1's.

    (b) Check your answer by an alternative computation.

16. (a) Use Theorem 7.4 to compute the number of legitimate codewords of length n from the alphabet $\{0, 1, 2\}$ if a codeword is legitimate if and only if it has exactly five 1's.

    (b) Check your answer by an alternative computation.

17. (a) Suppose that n children are born to a family. Use Theorem 7.4 to compute the number of ways the family can have exactly 2 boys.

    (b) Check your answer by the methods of Chapter 2.

18. (a) A psychic predicts a sequence of 4 elements, getting 2 right. What is the probability of getting at least this many right?

    (b) What is the probability of getting 3 or more right?

    (c) What is the probability of getting exactly 3 right? (Is there a problem with your answer? Explain.)

19. In a wine-tasting experiment, a taster is told that there will be 5 different wines given to him. After each, he guesses which of the 5 it was, making sure never to repeat a guess. He gets 3 right. What is his probability of getting at least 3 right if he is guessing randomly?

20. Write an expression for the probability that in a sequence of 7 random digits chosen from 0, 1, 2, ..., 9, exactly 2 of the digits will not appear.

21. In a genetics experiment, each mouse in a litter of n mice is classified as belonging to one of M genotypes. What is the probability that exactly g genotypes will be represented among the n mice?

22. Use Theorem 7.5 to find the number of families of 10 children that have an even number of boys. Check your answer by direct computation.

23. Use Theorem 7.5 to find the number of 8-digit sequences from the alphabet $\{0, 1, 2\}$ that have an odd number of 1's. Check your answer by direct computation.

24. Find the number of RNA chains of length 8 that have no U's and an even number of G's.

25. Give an alternative proof of Theorem 7.4 by using mathematical induction.

26. Use Theorem 7.4 to verify Equation (7.16).

27. In Exercise 27, Section 7.1, show that the number of ways to place the CDs so that exactly m players are empty is given by

$$\binom{n}{m} \sum_{i=0}^{n-m} (-1)^i \binom{n-m}{i} (n-m-i)^d.$$

28. Use Theorem 7.4 to verify (7.18).

29. Suppose that $P_m(c,n)$ is the probability that exactly m cells will be empty if n distinguishable balls are distributed into c distinguishable cells.

    (a) Show that
    $$P_m(c,n) = \binom{c}{m}\left(1-\frac{m}{c}\right)^n P_0(c-m,n).$$

    (b) Derive (7.18) from the equation for $P_0(c-m,n)$.

30. Let e_m^* be the number of elements of the set A having at least m of the properties $a_1, a_2, \ldots, a_r$. Show that
    $$e_m^* = s_m - \binom{m}{m-1}s_{m+1} + \binom{m+1}{m-1}s_{m+2} \mp \cdots + (-1)^p\binom{m+p-1}{m-1}s_{m+p} \pm \cdots + (-1)^{r-m}\binom{m+r-m-1}{m-1}s_r.$$

31. Suppose that $E_1, E_2, \ldots, E_r$ are events, that $p_{i_1 i_2 \cdots i_t}$ is the probability that events E_{i_1}, E_{i_2}, $\ldots$, E_{i_t} all occur, and that $S_t = \sum p_{i_1 i_2 \cdots i_t}$, where the sum in question is taken over all t-element subsets $\{i_1, i_2, \ldots, i_t\}$ of $\{1, 2, \ldots, r\}$. In terms of the S_t, derive expressions for

    (a) The probability that exactly m of the events occur;

    (b) The probability that at least m of the events occur.

32. In Exercise 8, Section 7.1, how many cars have at least 2 of the defects in question?

33. In Exercise 9, Section 7.1, how many students are taking at least 1 of the subjects in question?

34. Compute the number of RNA chains of length 10 with at least 2 U's.

35. Compute the number of legitimate codewords of length 7 from the alphabet $\{0, 1, 2\}$, where a codeword is legitimate if and only if it has at least three 1's.

36. Compute the number of permutations of $\{1, 2, 3, 4, 5\}$ in which at least three integers are in their natural position.

37. Suppose that B' is the complement of the $n \times m$ board B, $n \leq m$. If $j \leq n$, find a formula for $r_j(B)$ in terms of the numbers $r_k(B')$ which generalizes the result of Equation (7.11).

38. Use the result of Exercise 37 to show that
    $$R(x,B) = x^n R\left(\frac{1}{x}, B'\right).$$

39. (a) If $E(x)$ is the ordinary generating function for the sequence e_0, e_1, e_2, $\ldots$ and the e_i are defined as in Example 7.11, what is $E(1)$?

    (b) Find a formula for $E(1)$ that holds in general.

REFERENCES FOR CHAPTER 7

Adleman, L. M., and Huang, M.-D., *Primality Testing and Two Dimensional Abelian Varieties over Finite Fields*, Lecture Notes in Mathematics, 1512, Springer-Verlag, Berlin, 1992.

Adleman, L. M., Pomerance, C., and Rumely, R. S., "On Distinguishing Prime Numbers from Composite Numbers, *Ann. Math., 117*, (1983), 173–206.

Agrawal, M., Kayal, N., and Saxena, N., "PRIMES Is in P," Preprint, Aug. 6, 2002. http://www.cse.iitk.ac.in/primality.pdf.

Anshel, I., Anshel, M., and Goldfeld, D., "An Algebraic Method for Public-Key Cryptography," *Math. Res. Lett., 6* (1999), 287–291.

Barton, D. E., "The Matching Distributions: Poisson Limiting Forms and Derived Methods of Approximation," *J. Roy. Statist. Soc., 20* (1958), 73–92.

Berge, C., *Principles of Combinatorics*, Academic Press, New York, 1971.

Birkhoff, G. D., "A Determinant Formula for the Number of Ways of Coloring a Map," *Ann. Math., 14* (1912), 42–46.

Cohen, D. I. A., *Basic Techniques of Combinatorial Theory*, Wiley, New York, 1978.

De Moivre, A., *The Doctrine of Chances*, private printing, London, 1718.

Diffie, W., and Hellman, M. E., "New Directions in Cryptography," *IEEE Trans. Info. Theory, 22* (1976), 644–654.

Feller, W., *An Introduction to Probability Theory and Its Applications*, 3rd ed., Wiley, New York, 1968.

Goldstein, L. J., Schneider, D. I., and Siegel, M. J., *Finite Mathematics and Its Applications*, 7th ed., Prentice Hall, Upper Saddle River, NJ, 2001.

Goldwasser, S., and Kilian, J., "Almost All Primes Can Be Quickly Certified," Proceedings of Annual ACM Symposium on Theory of Computing, 1986, 316–329.

Hall, M., *Combinatorial Theory*, 2nd ed., Wiley, New York, 1986.

Hardy, G. H., and Wright, E. M., *Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, New York, 1980.

Irwin, J. O., "A Unified Derivation of Some Well-Known Frequency Distributions of Interest in Biometry and Statistics," *J. Roy. Statist. Soc., Ser. A, 118* (1955), 389–404.

Koblitz, N., *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994.

Liu, C. L., *Topics in Combinatorial Mathematics*, Mathematical Association of America, Washington, DC, 1972.

Miller, G. L., "Riemann's Hypothesis and Tests for Primality," *J. Comput. Sys. Sci., 13* (1976), 300–317.

Mizrahi, A., and Sullivan, M., *Finite Mathematics; An Applied Approach*, Wiley, New York, 1999.

Parzen, E., *Modern Probability Theory and Its Applications*, Wiley, New York, 1992.

Rabin, M. O., "Probabilitic Algorithm for Testing Primality," *J. Number Theory, 12* (1980), 128–138.

Reingold, E. M., Nievergelt, J., and Deo, N., *Combinatorial Algorithms: Theory and Practice*, Prentice Hall, Englewood Cliffs, NJ, 1977.

Rhee, M. Y., *Cryptography and Secure Communications*, McGraw-Hill, New York, 1993.

Rivest, R. L., Shamir, A., and Adleman, L. M., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM, 21* (1978), 120–126. (See also U.S. Patent 4,405,829, 1983.)

ROTA, G. C., "On the Foundations of Combinatorial Theory. I. Theory of Möbius Functions," *Z. Wahrscheinlichkeitsth. Verw. Geb., 2* (1964), 340–368.

SCHNEIER, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Wiley, New York, 1995.

SEBERRY, J., and PIEPRZYK, J., *Cryptography: An Introduction to Computer Security*, Prentice Hall, Englewood Cliffs, NJ, 1989.

SHEN, A., "Probabilistic Proofs," *The Mathematical Intelligencer, 20* (1998), 29–31.

SHOR, P. W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Computing, 26* (1997), 1484–1509.

SOLOVAY, R., and STRASSEN, V., "A Fast Monte-Carlo Test for Primality," *SIAM J. Computing, 6* (1977), 84–85.

STALLINGS, W., *Cryptography and Network Security: Principles and Practice*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1999.

UTTS, J. M., "Replication and Meta-Analysis in Parapsychology," *Statistical Science, 6* (1991), 363–403.

VERNON, P. E., "The Matching Method Applied to Investigations of Personality," *Psychol. Bull., 33* (1936), 149–177.

VILENKIN, N. YA., *Combinatorics*, Academic Press, New York, 1971. (Translated from the Russian by A. Shenitzer and S. Shenitzer.)

WHITNEY, H., "A Logical Expansion in Mathematics," *Bull. Amer. Math. Soc., 38* (1932), 572–579.