Contents

Lecture Notes for 21-228: *Discrete Mathematics*

Michael H. Albert

Chapter 1

Basic Enumeration

1.1 What is counting?

Counting is, perhaps, the origin of mathematics. It is something which we learn as children and give little thought to thereafter. But occasionally, counting problems arise which go beyond the basic counting skills which we acquired in the nursery. For example:

> *How many ways are there to get two pair at straight poker? (perhaps more importantly, how does this compare with the total number of possible hands?)*
>
> *How many possible rankings are there of 10 football teams?*
>
> *What are the chances of any particular ticket winning in the lottery?*

These are somewhat frivolous examples but there are also significant problems of this type. For example, to determine the efficiency of a computer program which sorts a data set it is critical to know just how many different possible initial orderings of the data set there are. If the orderings are unconstrained then this is an easy problem in counting, but if there are certain restrictions arising from the way in which the data was produced, the problem may be much more difficult.

So to begin, we should have a definition of just what it means to count – at least that is how a mathematician would like to begin. Specifically, we wish to know in formal terms just what we mean when we say that a set

has exactly 17 elements.

Notation: If n is a natural number, then:

$$[n] = \{1, 2, \ldots, n\}.$$

For the record, we do allow 0 as a natural number. After all, this is a book concerned with counting and 0 can well be the answer to a problem in counting (for example: "how many $1000 bills are there in my wallet?") Of course [0] is the empty set – the prototypical set with exactly 0 elements, just as [5] can be thought of as the "standard" set with 5 elements.

This all suggests the following definition:

Definition 1 *Let n be a natural number. A set A has* **cardinality** *n (or more simply, the number of elements in A is n) if there exists a bijection*

$$f : [n] \to A.$$

If A has cardinality n for some n, then we say that A is a **finite set**.

If A has cardinality n we would like to record this fact with a piece of notation like $|A| = n$ (read "the cardinality of A is equal to n".) This particular choice of notation would however be most unfortunate if there was any possibility that we might find a set A with the property that it had cardinality 2,343 and also cardinality 2,761. Our experience of counting tells us that this should not be so (if you count a pile of stones twice and get different answers your immediate reaction is to assume either that one of the counts was in error, or that someone has been adding or removing stones while you weren't looking.) We now record this little fact, and leave the work of proving it to you.

Theorem 2 *Let A and B be finite sets.*

1. *If $|A| = n$ and $|A| = m$ then $n = m$.*
2. *There is an injective function from A to B if and only if $|A| \leq |B|$.*
3. *There is a surjective function from A to B if and only if $|A| \geq |B|$.*

Henceforth we will extend our notation even further and use $|A|$ to stand for the unique positive integer n such that there is a bijection from A to $[n]$ (only in the case where A is a finite set of course.)

From the definition we see that "counting the number of elements" in a set involves determining a suitable value for n above, and hence either explicitly or implicitly constructing a suitable bijection. Often, for the sake of variety, we disguise questions which ask for the cardinality of a finite set in the form "In how many ways ..."

Example 1 *A penny, nickel, dime, and quarter are flipped. How many ways are there of getting exactly 2 heads?*

Solution: We will explicitly list the outcome of such coin flips as a sequence like THHH which would mean that the penny showed tails, and the remaining coins showed heads. With this notation, the set of acceptable outcomes is:

$$\{\text{TTHH, THTH, THHT, HTTH, HTHT, HHTT}\}$$

So there are exactly 6 ways of getting 2 heads. ■

This may well be the last time in this book when we explicitly enumerate the outcomes of an event. Part of the purpose of studying counting techniques is to be able to avoid such explicit listing, which rapidly becomes tedious as the number of outcomes increases.

Example 2 *Balls numbered 0, 1, 2, ..., 9 are placed in an urn. Four balls are drawn, one at a time, and replacing each ball in the urn after it has been drawn. How many possible outcomes are there?*

Solution: Consider a typical outcome (balls listed in the order in which they are drawn):

$$1, 3, 7, 8$$

Except for the commas, such an outcome looks like a four digit number. This leads to the immediate realization that to every integer between 0 and 9999 there corresponds a unique outcome to the experiment, obtained by writing the number as a 4 digit number (possibly with leading 0's), and inserting commas. So the number of outcomes is the same as the number of integers in this range, that is, 10,000. ■

The previous solution contains an important idea – that of a *correspondence*. The next section begins the actual study of counting techniques by bringing this idea to the fore.

1.1.1 Exercises

1. If n and m are natural numbers, and $n \leq m$, then what is
$$|\{n, n+1, \ldots, m\}|?$$
2. How many positive integers less than 1000 are multiples of 3? In general, how many positive integers less than n are multiples of k?
3. What is the total number of possible outcomes when a red and a green 6 sided die are rolled? What if two outcomes are considered the same if the numbers showing are the same (i.e. red 6 and green 5 is not distinguished from red 5 and green 6)?
4. In example 2 what is the total number of possible outcomes if the balls are not replaced after being drawn?
5. How many ways are there to deal two cards from the deck and get a pair?
6. Prove Theorem 2 (there are several subtle points involved particularly in the first part – induction is required).
7. Suppose that A and B are finite sets, and that $f : A \to B$ is a function with the property that for each $b \in B$ there are exactly 2 elements of A which are mapped to b by f. Prove that $|A| = 2|B|$.
8. Prove that the set of all natural numbers is *not* a finite set.

1.2 The correspondence principle

If there is a bijection between two finite sets A and B then they have the same number of elements. This trivial statement is in fact an extremely important observation which makes the task of enumerating finite sets much easier. In many circumstances, when asked "How many elements does A have?" it will prove to be easier to find a set B in bijective correspondence with A, whose cardinality is known, or at least is easily computed.

The statement above goes by the name of *the correspondence principle.* We will use it implicitly many times. For example, when we consider the problem of counting the number of r element subsets of an n element set, it will not matter which particular n element set is in question. Because there is a bijection between any two n element sets, and because such a

bijection induces a bijection between the r element subsets of the two sets, the number of r element subsets of any two n element sets are the same.

So for example, the number of 5 element subsets of [52] is equal to:

$$\binom{52}{5} = 2598960,$$

and this is the same as the total number of possible poker hands, since a poker hand just consists of a 5 element subset of the deck of 52 cards. The notation $\binom{n}{r}$ in general is used to denote the number of r element subsets of an n element set. It will not be long before we derive a formula for its value.

Example 3 *Show that the number of subsets of* $[n]$ *(or of any* n *element set) is* 2^n.

Solution: We first begin with a correspondence between the collection of all subsets of $[n]$ and the collection of all sequences of 0's and 1's of length n (the sequences 000, 001, 010, 011, 100, 101, 110, 111 are all such sequences of length 3). Such sequences are called *binary sequences of length* n.

To specify a binary sequence of length n we must determine whether the ith digit is to be 0 or 1, for each i between 1 and n. Given a subset $A \subseteq [n]$, we associate a sequence $s(A)$ whose ith digit is 1 if $i \in A$ and whose ith digit is 0 if i is not a member of A. For example the subset $A = \{1, 3, 6\}$ of [7] is given the associated sequence:

$$s(A) = 1, 0, 1, 0, 0, 1, 0.$$

It should be clear that this specifies a bijection between the collection of subsets of $[n]$ and binary sequences of length n. So the desired correspondence exists.

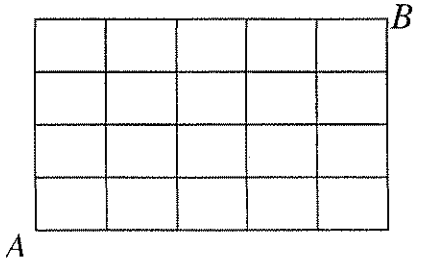
Now we observe that there is an obvious bijection between the binary sequences of length n, and the integers between 0 and $2^n - 1$ inclusive, which is obtained by simply viewing a sequence as standing for the binary representation of an integer in this range (possibly padded with some leading 0's). That is, we map the sequence $s = (s_1, s_2, \ldots, s_n)$ to the integer

$$2^{n-1}s_1 + 2^{n-2}s_2 + \cdots + 2^{n-i}s_i + \cdots + 2s_{n-1} + s_n.$$

Since there are 2^n integers in this range, there are 2^n subsets of an n element set.

Another way to reach this answer is to let a_n denote the number of binary sequences of length n. To each binary sequence of length $n-1$ there correspond 2 binary sequences of length n obtained by appending a 0 or a 1 respectively to the sequence. That is, the map from the set of binary sequences of length n to those of length $n-1$ specified by the rule "delete the last symbol" is exactly two to one. So for each n, $a_n = 2a_{n-1}$. Together with the obvious fact that $a_1 = 2$, and induction, this implies that $a_n = 2^n$. We will see much more of this kind of analysis when we discuss recurrences. ∎

Example 4 *Show that there is a correspondence between the number of routes from A to B in the grid below, traveling only along roads leading north or east, and the number of 4 element subsets of a 9 element set.*



Solution: Any route will be 9 blocks long – 4 of these blocks will be "northward". So the correspondence will be to associate to a route, the positions of the 4 northward blocks (giving a 4 element subset of [9]). ∎

1.2.1 Exercises

1. Describe a natural correspondence between the strictly increasing sequences of integers between 1 and 100 inclusive of length 17, and 17 element subsets of $\{1, 2, ..., 100\}$.

2. Describe a natural correspondence between the strictly increasing sequences of integers between 1 and 100 inclusive of length 17, and sequences of 17 positive integers whose sum is less than or equal to 100.

3. Describe a correspondence between sequences of length n from

   $$\{1, 2, \ldots, 9\}$$

   which do not begin with 1, and do not contain consecutive equal numbers, and arbitrary sequences of length n from $\{1, 2, \ldots, 8\}$.

4. Describe a correspondence between the set of binary sequences of length n which contain exactly one successive pair a_k, a_{k+1} of the form 0, 1, and the set of solutions in non-negative integers to the equation $X_1 + X_2 + X_3 + X_4 = n - 2$.

5. Describe a natural correspondence between the set of ways to distribute \$100 between four people (in multiples of \$1), and the set of 3 element subsets of [103].

6. Show that the function between subsets of $[n]$ and binary sequences of length n defined in Example 3 is a bijection. (Hint: The easiest way to do this may be to show that it has an inverse).

7. What is the number of routes between A and B in Example 4? (It may be helpful to solve some easier versions of this problem first and look for a pattern).

8. Let n be a positive integer. Show that the number of subsets of $[n]$ whose cardinality is even is equal to the number of subsets of $[n]$ whose cardinality is odd.

9. Consider the set S of all sequences of positive integers from 1 to 6. Let:

$$\begin{aligned} S_6 &= \{s \in S : \text{the sum of } s \text{ is } 6\} \\ S_7 &= \{s \in S : \text{the sum of } s \text{ is } 7\}. \end{aligned}$$

Prove that $|S_7| = 2|S_6| - 1$. This means that there are almost twice as many ways to roll a total of 7 at some point in a sequence of throws of a die, as there are ways to roll a total of 6. Generalize to sequences of integers from $[n]$ (Here the relationship between the corresponding set, call it say S_n and S_{n+1} is sought.)

10. Let n be a positive integer. Show that the number of ways to write n in the form:

$$n = a_1 + a_2 + a_3 + \cdots + a_k,$$

where

$$\begin{aligned} a_1 &\geq a_2 + a_3 + \cdots a_k \\ a_2 &\geq a_3 + a_4 + \cdots a_k \\ &\vdots \\ a_{k-1} &\geq a_k \end{aligned}$$

Is the same as the number of ways to write n in the form:

$$n = b_1 + b_2 + \cdots b_m$$

where:

$$b_1 \geq b_2 \geq \cdots \geq b_m$$

and each b_j is a power of 2. For example, with $n = 7$, the two sets of representations are:

$$7, 6+1, 5+2, 4+3, 5+1+1, 4+2+1;$$

and

$$\begin{array}{lll} 4+2+1, & 4+1+1+1, & 2+2+2+1, \\ 2+2+1+1+1, & 2+1+1+1+1+1, & \\ 1+1+1+1+1+1+1 & & \end{array}$$

each of which has 6 elements.

1.3 Two rules of counting

There are really only two fundamental rules which are applied when solving problems involving enumeration, the rule of sum, and the rule of product. Actually, there is really only one rule, but in practice we tend to view repeated addition as multiplication, which gives the second rule. The first rule is referred to as *the rule of sum*

Theorem 3 *If A and B are disjoint finite sets, then $|A \cup B| = |A| + |B|$ that is, the number of elements in the union of A and B is the sum of the number of elements in A and the number of elements in B.*

Proof: Recall that two sets are disjoint if their intersection is empty, or equivalently, there does not exist any element belonging to both the sets. Let $n = |A|$ and $m = |B|$. Let $f : A \to [n]$ and $g : B \to [m]$ be bijections. We define a function $h : A \cup B \to [n+m]$ as follows:

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \\ n + g(x) & \text{if } x \in B \end{cases}$$

The function h is well-defined because A and B are disjoint, and it is easy to check that it is a bijection. ∎

Example 5 *A red die and a green die are rolled. In how many ways can we get a total of 7 or 11?*

Solution: We just add the number of ways to get a total of 7 to the number of ways to get a total of 11, since the two results cannot occur simultaneously, and therefore represent disjoint sets of outcomes. To get a 7, we can get any of the numbers 1 through 6 on the red die, and then 7 minus that number on the green die. So there are 6 outcomes totalling 7. To get an 11 we must get a 5 or a 6 on the red die, and a 6 or a 5 on the green die, i.e. there are two outcomes totalling 11. So the total number of ways to get 7 or 11 is $6 + 2 = 8$. ∎

The following generalization of the rule of sum (which goes by the same name) is proved by induction (on the number of sets).

Theorem 4 *Let $A_1, A_2, \ldots A_n$ be pairwise disjoint finite sets. Then:*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

The proof is left as an exercise.

Remark: Whenever we have an associative operation (such as sum, product, union, or intersection) which we wish to apply to a list of n elements, we denote the result by the operation symbol and an indexed form of the list. This was used above for union. The symbol used for sum in this context is Σ, and for a product we use Π.

Example 6 *A red die and a green die are rolled. In how many ways can it occur that the number which appears on the green die is smaller than the number which appears on the red die?*

Solution: There are 6 possible outcomes of the roll of the red die, namely the numbers 1 through 6. If a 1 appears, then no roll of the green die will be smaller, if a 2 appears then 1 outcome (a "1") is smaller, ..., and if a 6 appears on the red die, then 5 outcomes will be smaller. Since the 6 possible outcomes for the red die represent disjoint sets, the total number of good outcomes is $0 + 1 + 2 + 3 + 4 + 5 = 15$. ∎

This last example illustrates that the application of the rule of sum really amounts to counting by cases.

Example 7 *A red die and a green die are rolled. In how many ways can it occur that the number which appears on the green die is different from the number which appears on the red die?*

Solution: There are 6 possible outcomes of the roll of the red die. No matter what the outcome, there are 5 allowable outcomes for the roll of the green die. So by the generalized rule of sum, there are $5+5+5+5+5+5 = 30$ good outcomes. ∎

In the last example above, we had an application of the rule of sum which involved the repeated addition of the same number. This process usually goes by the name of multiplication. So we have *the rule of product* which states that given two events A and B, if the number of ways in which B can occur is independent of the outcome of A, then the number of ways in which A and B occur is the product of the number of ways in which A can occur, and the number of ways in which B can occur, for any particular outcome of A. Stating this rule formally seems to be somewhat awkward, but we try to do so in the next theorem.

Theorem 5 *Let $E \subseteq A \times B$ be a subset of the cartesian product of two finite sets. For each $a \in A$ define:*

$$E_a = \{(a,b) : (a,b) \in E\} = E \cap (\{a\} \times B).$$

Suppose that for some n and every $a \in A$, $|E_a| = n$. Then:

$$|E| = |A| \times n.$$

Proof: Exercise ∎

Neither the informal, nor the formal statement of the rule of product is particularly illuminating. The following examples should serve to explain it better:

Example 8 *What is the total number of possible outcomes when a red die and a green die are rolled?*

Solution: There are 6 possible outcomes for the roll of each die, and these are independent of one another (i.e. the outcome of the roll of the red die does not affect the number of possible outcomes of the role of the green die), so by the rule of product there are $(6)(6) = 36$ possible outcomes. ∎

Example 9 *Two cards are drawn from a deck. In how many ways can a pair be obtained?*

Solution: No matter which card is drawn first (52 possibilities), there are 3 cards available to make a pair, so the total number of possible outcomes is (52) (3) = 156. ∎

Note, that here and henceforth the word "drawing" refers to an ordered selection. That is, both the things drawn and the order in which they appear are to be considered significant (think of a sweepstakes "drawing" for third then second then first prize – presumably the people involved will be interested in which prize they receive!)

There is a natural generalization of the rule of product when more than two events occur – this requires the number of possible outcomes of each event to be independent of the outcomes of the prior events. We illustrate this form of the rule by example only.

Example 10 *I have seven presents to give to my niece. We will be visiting for a week, and I will give her one present each day. In how many ways can I do this?*

Solution: This time the solution requires repeated application of the rule of product. On the first day, I have seven choices for which present to give. No matter which choice I make, I will have six presents left, and the number of ways I can distribute these does not depend on which present I gave first. This argument can be repeated for the next day etc. So I can give my niece her presents in

$$7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5040$$

different ways. ∎

1.3.1 Exercises

1. How many ways are there to deal two cards which total 15 from a deck (all face cards count as 10, aces count as 1)?

2. Each of 3 people chooses a lunch from among 7 possible choices. In how many ways is this possible? How many ways are there for them to make 3 different choices? How many ways are there for them to make exactly 2 different choices?

3. How many ways are there to draw five cards from a standard deck? How many ways are there to draw five cards from a standard deck without obtaining a pair?

4. Let A and B be finite sets. If $|A|$ and $|B|$ are known, but no other information about the sets is available, is it possible to calculate $|A \cup B|$? What if $|A \cap B|$ is also known?

5. How many positive integers less than 1,000 are divisible either by 2 or by 3?

6. Prove Theorem 4.

7. Prove Theorem 5. (Hint: Use the generalized rule of sum, and the fact that for $a \neq a'$, the sets E_a and $E_{a'}$ are disjoint)

1.4 Fundamental counting functions

So far, we have amassed a principle (correspondence) and two rules (sum and product) which enable us to count the number of elements in finite sets. These are the basic tools of the subject of enumeration, and in theory we really require nothing else – almost all the subsequent problems in this book could be solved by appeal only to these three facts. However, the task of counting will be much simplified if we have available the solutions to some basic counting problems which can be put together using the rules to solve more complicated problems. Three particular problems arise again and again: counting sequences, counting permutations, and counting subsets. We now deal with each of these in turn.

Definition 6 *A* **sequence** *of length r (or an r-sequence) from a set A is a list $a_1, a_2, \ldots, a_r$ of elements of A. Two sequences $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_r$ are equal if $a_j = b_j$ for all j between 1 and r.*

We often imagine constructing r-sequences from A by the process of choosing their elements in succession. That is, the elements of A are thrown into an urn, and r of them are withdrawn, one at a time, and replacing each element in the urn after it is drawn. If the outcome of such an experiment is recorded, we will see a sequence from A. The question arises: what is the total number of r-sequences from a finite set A?

Theorem 7 *Let A be a finite set of cardinality n. The number of r-sequences from A is n^r.*

Proof: Consider the method of constructing sequences outlined above. Choosing an r-sequence from A involves choosing an element from A and

repeating this r times. At each repetition, there are n elements available to choose from (since elements are replaced in the urn each time they are chosen), so by the rule of product, the total number of ways to carry out these choices is

$$n \times n \times n \times \cdots \times n = n^r.$$

■

By convention, and because it agrees with the above formula, the number of 0-sequences from any set is taken to be 1 (another way to justify this is to assert, that just as there exists one and only one empty set, there exists one and only one empty list).

In the construction procedure above, what happens if we do not allow the elements to be replaced in the urn once they are chosen? In this case, the sequences which arise will not contain any repetitions. Such sequences are called permutations.

Definition 8 *A* **permutation** *of length r (or r-permutation) from a set A is an r-sequence from A which does not contain any repetitions (i.e. $a_1, a_2, \ldots, a_r$ is an r-permutation if $1 \leq i < j \leq n$ implies $a_i \neq a_j$). If A has cardinality n, then a* **permutation** *of A is an n-permutation from A.*

Again, the question arises: what is the total number of r-permutations from A?

Theorem 9 *Let A be a finite set of cardinality n. The number of r-permutations from A (which is often denoted $P(n,r)$) is*

$$\prod_{k=1}^{r}(n-k+1) = n(n-1)(n-2)\cdots(n-r+1)$$

.

Proof: We return to the construction procedure. Again, a permutation is constructed in r steps. This time however, at the kth step, $k-1$ elements have already been removed and are no longer available, leaving $n-k+1$ elements in the urn. As this number does not depend on which $k-1$ elements have been removed, the rule of product still applies and yields the number above. ■

Again, by convention, the number of 0-permutations is taken to be 1. Notice that the formula above already illustrates that if A has n elements then there are no r-permutations of A for $r > n$ (since we run out of elements).

When $r > n$ there is a factor of 0 in the product above, and hence $P(n,r) = 0$. The special case when $r = n$ is particularly important:

$$P(n,n) = n(n-1)(n-2)\cdots(3)(2)(1).$$

This product is denoted $n!$. This notation makes it possible to condense the formula for $P(n,r)$ somewhat, at least for the "sensible" cases with $0 \leq r \leq n$:

$$P(n,r) = \frac{n!}{(n-r)!} \quad \text{if } 0 \leq r \leq n.$$

In computation, this is often the most useful form, but it is important to remember that $P(n,r)$ makes sense for all non-negative integers r, it just happens to equal 0 for $r > n$.

In many card games one is dealt a hand from a 52 card deck. Typically, the order in which one receives the cards is irrelevant – all that matters is the cards received. This is true for example in poker or bridge – but not in most games of solitaire. A collection of elements without repetitions, in which order is irrelevant is simply a set.

Definition 10 *Let A be a set. An r-**subset** of A is any subset of A whose cardinality is r. If A has cardinality n then the number of r-subsets of A is denoted by $C(n,r)$ or $\binom{n}{r}$ (read "n **choose** r").*

By now you should be able to judge what comes next:

Theorem 11 *Let A be a set of cardinality n. The number of r-subsets of A is:*

$$\binom{n}{r} = \frac{P(n,r)}{r!}.$$

Proof: Until now we have not needed any real subtlety in applying the rule of product to obtain counting functions. Now things have changed. First let us aim to obtain the equivalent formula:

$$P(n,r) = \binom{n}{r} r!$$

which does not involve division. To prove this formula it suffices to provide a method of constructing all the r-permutations of A which involves first choosing an r-subset. This is not so hard.

- Choose an r-subset of A,

- Choose an arbitrary permutation of this subset.

Clearly every r-permutation of A is constructed once and only once by this procedure. In the analogy with a sweepstakes drawing mentioned earlier it amounts to first choosing the set of winning tickets, and then choosing from among them which win the first prize, second prize, and so on. By the definition of $\binom{n}{r}$, the first part of the procedure can be carried out in $\binom{n}{r}$ ways. Once we have an r-subset, there are $r!$ permutations of it, so the second part of the procedure can always be carried out in $r!$ ways. By the rule of product:

$$P(n,r) = \binom{n}{r} r!$$

as required. ∎

For the "sensible" values of r, that is $0 \leq r \leq n$ we have the formula:

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

which is most useful computationally. However, the form given in the theorem also applies when $r > n$ yielding the correct answer of 0.

The proof of Theorem 11 illustrates a "combinatorial" proof of an identity. Such a proof establishes that two quantities are equal by showing that they both represent the cardinality of the same finite set computed in different ways.

Now we can apply some of these results to "practical" problems.

Example 11 *How many poker hands are there? Of these, how many contain exactly one pair (and not three of a kind or 2 pair)?*

Solution: A poker hand is simply a 5 element subset of the 52 element set of cards in the deck. So there are $\binom{52}{5}$ different poker hands.

The problem of determining how many contain exactly one pair is a little more difficult. The methods used are typical of problems of this type. We intend to use the product rule so we need to divide the description of a hand containing exactly one pair into a number of stages. The first thing to recognize is that a hand which contains exactly one pair contains a pair, and then three other cards of differing ranks. So there are two steps in constructing such a hand:

- Determine the pair,

- Determine the other three cards.

How many ways are there to determine the pair? A pair is determined by its rank (2 through Ace) and which 2 suits the cards in the pair belong to. There are 13 possible ranks, and $\binom{4}{2} = 6$ possible suit selections. So the first part of constructing the hand can be carried out in $13(6) = 78$ different ways.

Now what about the other 3 cards? In order to avoid a card of the same rank as the pair, or another pair, these 3 cards must have 3 different ranks from the 12 remaining ranks. So the ranks of the cards can be determined in $\binom{12}{3} = 220$ ways. Once the ranks are determined, we must determine a suit for each card. This suit can be chosen in 4 ways. So there are $220(4^3) = 14080$ choices for the other 3 cards.

Why did we use the counting number for a subset (orderless) when we were choosing the 3 ranks, but for a sequence (order important) when we were choosing the suits? The important point here is that if we know only the three ranks, then a hand containing say a 4 of hearts, a jack of spades, and a 7 of hearts cannot be distinguished from a hand containing a jack of spades, a 7 of hearts, and a 4 of hearts. However, once we know the ranks (4, 7, jack), the order of the suit selection is important, because the hands above are different from the hand containing a 4 of spades, 7 of hearts, and jack of hearts.

Thus the total number of hands containing exactly one pair is:

$$78(14080) = 1,098,240$$

compared to

$$\binom{52}{5} = 2,598,960$$

total hands (or 42.2 % of all possible hands.)

Incidentally I find that the answer:

$$13\binom{4}{2}\binom{12}{3}4^3$$

for the second part is far more illuminating than the actual number – it practically (but not quite) contains an explanation of how it was obtained. ■

Example 12 *How many poker hands which contain exactly one pair consisting of a pair of jacks or better (queen, king, or ace)?*

Solution: We could start from scratch and solve the problem as above. However, a somewhat quicker method is to recognize that the number of hands containing any particular rank of pair (like a pair of jacks) must be 1/13 of the total number of hands containing exactly one pair. Since such hands never contain 2 pairs (by definition), the total number of such hands containing "jacks or better" is:

$$(4/13)13\binom{4}{2}\binom{12}{3}4^3 = 4\binom{4}{2}\binom{12}{3}4^3 = 337920.$$

■

Example 13 *Bob and Jenny's ice cream comes in 311 different flavors. How many different ways are there for 6 people to order a small or large cone? (One flavor of icecream per cone.)*

Solution: Each person has 622 alternatives (one for each flavor and size of cone). Since the order of selection is important (presumably!), and there is no restriction on duplication of selections, we have a sequence of length 6 from this 622 element set. So the total number of such orders is:

$$622^6 = 5.8 \times 10^{16}$$

■

Example 14 *How many different orders are possible if no 2 of the 6 people order the same flavor?*

Solution: This can be done either directly from the rule of product (622 possibilities for the first order, 620 for the second – since a flavor has been eliminated, 618, ...) giving:

$$622 \times 620 \times 618 \times 616 \times 614 \times 612 = 5.5 \times 10^{16}$$

or as follows.

Consider the sequences of flavors and sizes separately. Under the constraints of the problem there are $P(311, 6)$ allowable sequences of flavors (since we are not allowed repetition of flavor), and 2^6 sequences of sizes (since we do allow repetition of sizes). Together these account for:

$$P(311, 6)2^6 = 5.5 \times 10^{16}$$

possible outcomes. ■

Example 15 *How many possible arrangements are there of the letters of the word "example"? How many of these do not contain consecutive vowels?*

Solution: If all the letters of the word "example" were distinct the answer would just be 7!. However, we cannot distinguish the 2 e's from one another, so this is not correct. Very simply the idea is to imagine that we have 7 slots into which we intend to insert these 7 letters. First we insert the 2 e's. This can be done in $\binom{7}{2}$ ways since we just choose 2 slots for them. The remaining 5 letters are distinct, and can be arranged arbitrarily in the remaining 5 slots, so this can be done in 5! ways. So the total number of arrangements is $\binom{7}{2}5!$.

For the second part, first arrange the four consonants – this can be done in 4! ways. Now the vowels must be placed between the consonants, and no two vowels must be between the same pair of consonants. This means that there are 5 places to put the vowels (before the first consonant, between first and second, ..., after the fourth). Choose 2 of these 5 places in which to put the e's – this can be done in $\binom{5}{2}$ ways, and then choose one of the 3 remaining places for the a. The final answer is:

$$4!\binom{5}{2}3$$

■

An alternative approach to the second part of the last example is to first construct a template consisting of 4 C's and 3 V's in which no two V's are consecutive. This can be done in $\binom{5}{3}$ ways. Then replace the C's by the consonants from the word "example", and the V's by the vowels. This yields an additional pair of factors of 4! and $\binom{3}{2}$ – giving the same final answer.

1.4.1 Exercises

1. How many possible rearrangements are there of the letters in each of the following words?

   (a) abstruse

   (b) random

   (c) argyle

   (d) beekeeper

2. In the spring semester at NoWhere U., 250 students each enrolled in exactly 1 of 10 courses.

   (a) In how many ways is this possible?

   (b) How many ways are there for each course to get exactly 25 students?

3. How many rearrangements of the letters in the following words do not contain consecutive vowels?

   (a) mellow

   (b) aggravated

   (c) antidisestablishmentarianism

   (d) gorgonzola

4. Prove the following identities combinatorially (i.e. without using the explicit formulas for the functions involved, but rather by showing that the two sides of each equation are obtained by counting the number of elements in the same set in two different ways).

   (a) $P(n,r) = nP(n-1,r-1)$.

   (b) $\binom{n}{r} = \binom{n}{n-r}$.

   (c) $k\binom{n}{k} = n\binom{n-1}{k-1}$.

   (d) $\binom{n}{k}\binom{n-k}{l} = \binom{n}{l}\binom{n-l}{k}$

   (e) $\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}$

5. How many binary sequences of length 2, 3, 4, and 5 are there which do not contain a pair of consecutive 0's? You may have to do this by explicitly listing the elements of these sets. Suggest a relationship between these numbers and try to prove it.

1.5 Probability

As we have seen, many counting problems involve counting the number of elements in some particular finite subset of a finite set (for example the number of poker hands containing two pair). If the overlying set in question is a set of events, and if each of these events are equally likely, then there is a naturally associated notion of the probability of an event.

Definition 12 *Let U be a finite set of events, and suppose that each event in U is equally likely. If $A \subseteq U$ then we define* **the probability of** *A to be:*

$$p(A) = \frac{|A|}{|U|}.$$

What does the phrase *equally likely* mean? To answer that question would delve too deep into the foundations of the theory of probability. We content ourself with the pragmatic viewpoint (which, I am told, is called the Bayesian or personalist approach to probability) that if $|U| = N$ then the events in U are equally likely if you would be willing to bet \$1 that any particular one would occur provided that you would win at least $\$(N-1)$ if it did. However, it is an issue which one should pay attention to, as the following example shows:

Example 16 *Three identical coins are tossed simultaneously. What is the probability that all three will come up heads?*

Apparently there are only 4 outcomes, according to the number of heads (since the coins are identical we cannot distinguish between THT and HTT). One of these 4 outcomes is that all three coins will be heads, so the probability should be 1/4.

Experience and common sense tell us that this is not the case. The most natural line of reasoning which suggests this is to note that if the coins were marked in some way (so that they appeared to be identical but weren't), then in principle the outcomes THT and HTT could be distinguished from one another. In this case only 1 of 8 outcomes is three heads, yielding a probability of 1/8 – which agrees with experience. The process of marking the coins should not affect the probability that any one of them will come up heads, so the previous argument must be invalid.

The moral of this particular example is that in the macroscopic world at least, one should always treat distinct physical objects as if they were distinguishable from one another when determining probabilities. In quantum mechanics, there are particles for which this is not true, and for which the reasoning in the paragraph immediately following the example is correct.

Example 17 *A fair coin is flipped 10 times. What is the probability that exactly 5 heads will occur?*

Solution: Any sequence of 10 H's or T's is equally likely, so there are $2^{10} = 1024$ possible outcomes. To count the outcomes with exactly 5 H's

we observe that these correspond to the 5 element subsets of [10] (labeling the 5 places at which H's occur). So there are $\binom{10}{5} = 252$ such outcomes. Therefore the required probability is:

$$\frac{\binom{10}{5}}{2^{10}} = \frac{252}{1024} = \frac{63}{256} = 0.246$$

■

Example 18 *If you are dealt 6 cards from a well shuffled deck, what is the probability that they will all have different ranks?*

Solution: There are two equally correct ways to handle this problem. The first concentrates on the cards as they are dealt (i.e. takes order into account), and the second concentrates only on the final hand.

If we look at the cards as they are dealt, then the total number of equally likely outcomes is $P(52, 6)$ since we receive 6 cards, chosen from a 52 card deck. If all the ranks are to be different, then there are 52 possibilities for the first card, 48 for the second (since the other cards of the same rank as the first should be eliminated), 44 for the third, 40 for the fourth, 36 for the fifth, and 32 for the sixth. Thus the required probability is:

$$\frac{52(48)(44)(40)(36)(32)}{P(52,6)} = 0.345$$

On the other hand, it is clear that we are equally likely to receive any 6 element subset of the deck as our complete hand. With this model, the total number of outcomes is only $\binom{52}{6}$. Now to obtain a hand of the required type, we must choose 6 different ranks which can be done in $\binom{13}{6}$ ways, and then choose suits for each of the cards, which can be done in 4^6 ways (for an explanation of why we switch from an unordered to an ordered model here see Example 11). So the required probability is:

$$\frac{\binom{13}{6}4^6}{\binom{52}{6}} = \frac{7028736}{20358520} = 0.345$$

In fact the two fractions are exactly the same (as they should be) – in the first method both the numerator and the denominator are larger by a factor of 720. ■

Which method is better? It depends on the particular problem. In this case the first method seems simpler since we can use a direct application of

the rule of product in the numerator. However, with some other examples (e.g. calculating the probability of getting exactly one pair) the number of cards which one can receive at any point depends on which cards have already been received (in particular whether or not the pair has already been made), and it is not possible to use the first method at all, or it may be possible but extremely cumbersome (as an exercise, one could calculate the probability that a poker hand contains exactly one pair in this way.)

We finish with a classical example – the "birthday problem".

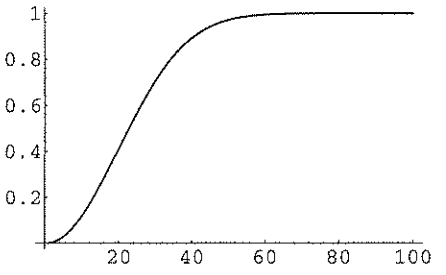
Example 19 *In a group of n people what is the probability that at least 2 people will have the same birthday? What is the smallest value of n for which this probability exceeds $1/2$?*

Solution: We must make some simplifying assumptions to do this problem. First, for simplicity we will assume that no one is ever born on Feb. 29. Next we assume that a person is equally likely to be born on any particular day of the year (both these assumptions are of course wrong – in particular, more people are born in September than in any other month, but they are near enough to the truth not to have a major effect on the final answer).

So among n people there are 365^n equally likely sets of birthdays. It seems to be hard to calculate directly the number of ways for at least 2 of them to have the same birthday, but it turns out that it is easy to calculate the number of ways for no 2 of them to have the same birthday – it is just $P(365, n)$ (if no 2 are to have the same birthday, then the list of the birthdays of all the people, will be an n-permutation of 365). Since the sum of the number of ways for at least 2 of them to have the same birthday and the number of ways for no 2 of them to have the same birthday must be the total number of outcomes (namely 365^n), there are $365^n - P(365, n)$ ways for at least two of them to have the same birthday. Therefore the probability of this event is:

$$p_n = \frac{365^n - P(365, n)}{365^n} = 1 - \frac{P(365, n)}{365^n}.$$

The graph below illustrates this probability.



In particular, $p_{22} = .476$, $p_{23} = .507$, so as soon as there are 23 or more people in a group the probability that two will have the same birthday is more than 1/2 (this does not change if we allow 366 possible birthdays). ■

1.5.1 Exercises

1. What is the probability of receiving poker hands of the following types?
   (a) two pair,
   (b) 3 of a kind,
   (c) full house (three of a kind and a pair),
   (d) straight (five cards of consecutive rank),
   (e) flush (five cards of the same suit).
2. A bridge hand consists of 13 cards from the standard 52 card deck. The "shape" of a bridge hand is the number of cards held in each suit, listed in decreasing order. Determine the probability of receiving a bridge hand of each of the following shapes when the cards are dealt from a well-shuffled deck:
   (a) 5, 4, 3, 1
   (b) 4, 3, 3, 3
   (c) 4, 4, 3, 2
   (d) 5, 3, 3, 2
   (e) 6, 5, 1, 1
   (f) 13, 0, 0, 0 (such a hand is typically reported several times a year – are these reports very likely to be accurate?)
3. A fair coin is tossed 10 times. What is the probability of not getting two heads in a row?

4. A ticket for the Pennsylvania lottery is a 7 element subset of [80]. Each Wednesday, an 11 element subset of [80] is determined, and a ticket wins if all the numbers on the ticket are among the numbers chosen. What is the probability that any particular ticket will win?

5. Let n be a positive integer. Suppose that two subsets A and B of $[n]$ are chosen independently, and so that any subset of $[n]$ is equally likely to be chosen. Show that the probability that $A \cap B = \emptyset$ is $3^n/4^n$. What is the probability that $A \cup B = [n]$?

6. A fair coin is tossed $2n$ times. What is the most likely number of heads to occur? What is the behavior of the probability of this event as n becomes large? What is the behavior of the probability that the number of heads will be within 10% of this value as n becomes large (this requires a computer calculation – or some fairly heavy duty mathematics).

7. (A non-problem) Try to convince yourself that it is reasonable to suppose that in a group of n unrelated people, the chances that two will have the same birthday will actually be higher than that given by the formula above due to the fact that not all birthdays are equally likely.

8. In the Birthday Problem we showed that fewer than 50% of the 23-sequences from [365] are permutations.. For an arbitrary integer n we can ask the question, what is the least value of k so that fewer than 50% of the k-sequences from $[n]$ are k-permutations? Investigate the behavior of this number as a function of n – in particular try to determine how quickly it grows (is it a linear function of n, or something like the logarithm, or is it somewhere in between?).

9. With reference to Example 16 is there any way to weight three coins (so that for each coin heads and tails do not occur with equal probability) in such a way that the four outcomes "no heads", "one head", "two heads", and "three heads" are equally likely?

1.6 Other counting problems

The counting functions for sequences, permutations, and subsets, also arise in another context, often called the "balls in boxes" model. Briefly, the idea is that we are given a set of r balls, and n boxes, labeled $1, 2, \ldots, n$. The problem is to determine how many ways there are to place the balls in the boxes subject to various restrictions.

Example 20 *If the balls are distinguishable (say by labels* $1, 2, \ldots, r$*), and any number of balls can go in a box; how many ways are there to place the balls in the boxes?*

Solution: The balls are distinguishable, so an arrangement corresponds to answering the questions "where does ball 1 go?", "where does ball 2 go?", ..., "where does ball r go?". There are n possibilities for each ball, so by the rule of product, there are n^r ways to place the balls.

Alternatively, we can see directly the correspondence between this set, and the set of r-sequences from $[n]$. Given a sequence $s_1, s_2, \ldots, s_r$ it corresponds to placing ball 1 in box s_1, ball 2 in box s_2, and so on. ∎

What happens if the boxes are small and can only hold 1 ball each?

Example 21 *If the balls are distinguishable (say by labels* $1, 2, \ldots, r$*), and only one ball can go in any box; how many ways are there to place the balls in the boxes?*

Solution: The same correspondence as in the second paragraph of the solution above illustrates that this situation amounts to counting the r-permutations of $[n]$. So the answer is $P(n, r)$.

Alternatively, we can argue as in the first paragraph above, and use the rule of product to obtain the same answer. ∎

Now what happens if we cannot distinguish the balls from one another?

Example 22 *If the balls are indistinguishable, and only one ball can go in any box; how many ways are there to place the balls in the boxes?*

Solution: An arrangement of the balls corresponds to choosing r boxes from among the n in which to place them. Since the order in which these choices are made does not effect the final outcome (because the balls are indistinguishable), the total number of ways to place the balls is just the number of r-element subsets of $[n]$, i.e. $\binom{n}{r}$. ∎

Well, we have used up our three counting functions, and it is clear that there is a case which we have not yet considered – indistinguishable balls and big boxes. Let us see what we can do with that.

Example 23 *If the balls are indistinguishable, and any number of balls can go in a box; how many ways are there to place the balls in the boxes?*

Solution: We begin by establishing an important correspondence:

> The answer to this problem is the same as the number of solutions to the equation
>
> $$X_1 + X_2 + \cdots + X_n = r$$
>
> where the X_i are integers and each $X_i \geq 0$.

The correspondence is easy – given an arrangement of the balls, all we need to know to determine it uniquely is the number of balls in each box (since the balls are indistinguishable). These n numbers must all be greater than or equal to 0 (a box can't contain a negative number of balls), and their sum must equal r (the total number of balls), so we have a solution to the equation above. Conversely, to any solution $(a_1, a_2, \ldots a_n)$ of the equation, there corresponds the arrangement of balls in which there are a_1 balls in box 1, a_2 balls in box 2, and so on.

Now we need to determine the number of solutions to the above equation. Imagine that we have a solution $(a_1, a_2, \ldots a_n)$. One way to represent this would be with a series of tick marks on a piece of paper. We would start with a_1 tick marks for the value of X_1, then place a dividing line, then a_2 tick marks, another dividing line, ..., a_{n-1} tick marks, a dividing line, and finally a_n tick marks (we don't need another dividing line since there is nothing left to follow). So we end up with r tick marks and $n-1$ dividing lines at certain points between them. If we use 1's to represent the tick marks, and 0's for the dividing lines then we have a binary sequence of length $n+r-1$ which contains exactly r 1's.

Conversely, any such sequence corresponds to a solution of the equation (just by counting the number of 1's between consecutive 0's). So we have yet another correspondence. But now we know the answer – there is a correspondence between such sequences and the r-subsets of $[n+r-1]$ (obtained by listing the positions of the 1's, so there are

$$\binom{n+r-1}{r}$$

such sequences, such solutions, and such arrangements of balls. ∎

There is one other counting problem that the function above solves – the number of *r-multisets* from an n-element set is $\binom{n+r-1}{r}$. A multiset is a list of elements, with repetitions allowed, and two multisets are equal if they contain the same elements, each repeated the same number of times. By now, the correspondence between these, and one of the sets above should be clear.

Example 24 *A total of 80 students registered for Discrete Mathematics. In how many different ways can they be assigned to 3 different sections, if two assignments are considered the same if they have the same number of students in each section?*

Solution: Let X_i stand for the number of students in the ith section ($i \in \{1,2,3\}$). Then an assignment of students corresponds to a solution to:

$$X_1 + X_2 + X_3 = 80$$

By the above, there are $\binom{82}{80}$ such solutions. ∎

Example 25 *How many ways are there to divide the students as above if no classroom can hold more than 50 students?*

Solution: We use the information which we have already, that in the unrestricted case there are $\binom{82}{80}$ possible assignments, and we subtract the number of assignments which have at least one class too large. Note that it is not possible for more than one class to be too large, so the events "section 1 too large", "section 2 too large", and "section 3 too large" are disjoint. By symmetry, all these sets have the same number of elements. So we only need to calculate the number of ways in which section 1 is made too large, multiply by 3, and subtract from the result above.

If section 1 has 51 or more students, then

$$X_1 = 51 + Y_1$$

where Y_1 is a non-negative integer. Therefore the number of arrangements in which section 1 is too large is equal to the number of solutions of:

$$\begin{aligned} (51 + Y_1) + X_2 + X_3 &= 80 \quad \text{or} \\ Y_1 + X_2 + X_3 &= 29 \end{aligned}$$

in non-negative integers. This is: $\binom{31}{29}$. So the total number of arrangements where no section has more than 50 students is:

$$\binom{82}{80} - 3\binom{31}{29}.$$

∎

When we study the principle of inclusion/exclusion we will see how to solve problems like the one above when more than one constraint can be violated.

Example 26 *Prove the identity:*

$$\binom{n+r-1}{r} = \sum_{j=0}^{r} \binom{n+r-j-2}{r-j}.$$

Solution: The left hand side is known to count the number of solutions of:

$$X_1 + X_2 + \cdots + X_{n-1} + X_n = r$$

in non-negative integers. These solutions break down into $r+1$ disjoint sets, according to the value of X_n which must be between 0 and r. For any particular value j of X_n, the number of solutions is

$$\binom{(n-1)+(r-j)-1}{r-j} = \binom{n+r-j-2}{r-j}$$

since there remain $n-1$ variables which must add up to $r-j$. Summing over the possible values of j establishes the result. ∎

The identity above does not look terribly natural, but by renaming some of the quantities involved it is equivalent to the far more natural identity:

$$\binom{m}{k} = \binom{m-1}{k} + \binom{m-2}{k-1} + \binom{m-3}{k-2} + \cdots + \binom{m-k}{1} + \binom{m-k-1}{0}.$$

1.6.1 Exercises

1. How many ways are there to distribute \$100 in \$1 bills among 4 people? What about \$100 in dimes?
2. How many binary sequences of length n are there with the following properties?
   (a) No 0's.
   (b) At most 3 0's.
   (c) At most 1 occurrence of 01.
   (d) At most 2 occurrences of 01.
3. (a) How many binary sequences of length n are there which contain exactly k 0's, but which do not contain consecutive 0's?
   (b) Using the above, write down a sum for the number of binary strings of length n which do not contain consecutive 0's.

(c) If f_n denotes the number of binary sequences of length n which do not contain consecutive 0's, then prove that

$$f_n = f_{n-1} + f_{n-2}.$$

4. Another combinatorial proof of the identity:

$$\binom{m}{k} = \binom{m-1}{k} + \binom{m-2}{k-1} + \binom{m-3}{k-2} + \cdots + \binom{m-k}{1} + \binom{m-k-1}{0}$$

can be obtained by partitioning the k-element subsets of $[m]$ in a fairly natural way and using the rule of sum. Find such a proof.

1.7 Explicit enumeration

In the previous sections we developed some techniques for enumerating finite sets without constructing explicit bijections. We now turn this idea around, and ask whether the enumerative techniques themselves give us information about how to construct bijections. There are several reasons for undertaking such a task. First of all, an explicit bijection between $[n]$ and some finite set A may yield information about the general structure of A. Secondly, it gives us a method for choosing a random element of A – just choose a random number from $[n]$ and apply the function. Such a facility can be useful in testing programs which operate with elements of A as input. Finally, it imposes an ordering on A, which may be useful in inductive arguments about elements of A.

We return to the three basic building blocks of counting – sequences, permutations, and subsets. To begin with sequences: how can we find an explicit bijection between $[n^k]$ and k-sequences from $[n]$? So we wish to associate a k-sequence from $[n]$ to each integer m between 1 and n^k. This turns out to be relatively easy - just write $m-1$ as a k digit number in base n (with leading 0's if necessary), and then add 1 to each digit. Let us agree to be satisfied with sequences from $\{0, 1, 2, \ldots, n-1\}$ in this section in order to make such modifications unnecessary. So for the sake of convenience we will define a bijection from the set $\{0, 1, \ldots, n^k - 1\}$ to the set of k-sequences from $\{0, 1, \ldots, n-1\}$.

How do we actually write a non-negative integer m in base n? We use the fact that:

$$m = \lfloor m/n \rfloor n + r \quad \text{for some } 0 \leq r < n$$

(the notation $\lfloor x \rfloor$ stands for the greatest integer which is less than or equal to x.) The units digit of m is the number r, the remainder on division of m

by n. We will denote this number r by $m \pmod n$. The rest of the number to the left is the base n representation of $\lfloor m/n \rfloor$. So we continue by finding the base n representation of $\lfloor m/n \rfloor$. In essence, we have defined a recursive procedure for writing m in base n. This procedure terminates when we have divided by n sufficiently often and we reach the point of trying to write 0 in base n (which is not too difficult). In order to ensure exactly k digits which we wish to do here, we may need to pad to the left with 0's. The easiest way to do this is to specify a function:

$\mathsf{Seq}[m, n, k]$:= Produce the rightmost k digits of m written in base n.

This is done by the recursive rules:

$$\begin{aligned} \mathsf{Seq}[m, n, 0] &:= () \\ \mathsf{Seq}[m, n, k] &:= \mathsf{Seq}[\lfloor m/n \rfloor, n, k-1],\ m \pmod n \end{aligned}$$

There are two questions to be answered at this point:

> Have we indeed defined a bijection from $\{0, 1, 2, \ldots n^k - 1\}$ to k-sequences from n?
>
> How difficult is it to evaluate the effect of this map?

The first part is proved inductively. Certainly $\mathsf{Seq}[m, n, 0]$ defines a bijection from $\{0\}$ to the single empty sequence. Now supposing that $\mathsf{Seq}[m, n, k]$ defines a bijection between $\{0, 1, 2, \ldots n^k - 1\}$ and k-sequences from n, we observe that the $k+1$ sequences from $[n]$ consist of all of the k sequences each followed by the digits $\{0, 1, \ldots n-1\}$. When $\mathsf{Seq}[m, n, k+1]$ is evaluated, the first n values are just the sequences:

$$\mathsf{Seq}[0, n, k], 0 \quad \text{through} \quad \mathsf{Seq}[0, n, k], n-1$$

Likewise the next n sequences are $\mathsf{Seq}[1, n, k]$ followed by 0 through $n-1$. So we see from the description of the $k+1$ sequences above, that we have defined a bijection.

Observe that to evaluate $\mathsf{Seq}[m, n, k]$ requires a fixed number of arithmetic operations plus an evaluation of $\mathsf{Seq}[\lfloor m/n \rfloor, n, k-1]$. So all together the number of operations performed is some constant times k. If we wanted just the representation of m without leading 0's, this would amount to a constant times the logarithm of m.

That example was fairly easy. We turn now to k-permutations of $[n]$. Again the nature of the computation of $P(n, k)$ suggests a recursive algorithm to solve the problem. Supposing that we have found a bijection from $P(n, k-1)$ to the $k-1$ permutations of $[n]$, we introduce $n-k+1$ new places for each,

to be filled with the $n-k+1$ possible final digits. Again for convenience we will take the domain of our bijection to be $\{0,1,\ldots,P(n,k)-1\}$.

A slight difficulty arises in that the set of final digits which may be used depends on which digits were used in the rest of the permutation. We deal with this as follows:

1. First map $m \in \{0,1,\ldots,P(n,k)-1\}$ to a sequence $a_1,a_2,\ldots,a_k$ where
$$0 \leq a_i \leq n-i.$$
2. Then map such sequences (which may contain repetitions) to permutations.

The first part is accomplished as follows:
$\mathtt{P1}[m,n,0] \quad := \quad ()$
$\mathtt{P1}[m,n,k] \quad := \quad \mathtt{P1}[\lfloor m/(n-k+1)\rfloor, n, k-1], m \,(\mathrm{mod}\, n-k+1)$

To map such a sequence $a_1,a_2,\ldots,a_k$ to a permutation, we begin with the whole list of elements which we have available – i.e. $[n]$. We construct a permutation by choosing the (a_1+1)st element of the list, deleting it, then choosing the (a_2+1)st element of the remaining list and so on until we are finished.

Finally we consider the problem of finding a bijection from $[\binom{n}{k}]$ to the set of k-elements subsets of $[n]$. Again, an identity, in this case:

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

provides a recursive construction. Formally, suppose that we have defined functions $f_{m,r}$ which are bijections from $[\binom{m}{r}]$ to the r element subsets of $[m]$ for each $m < n$. Then, recalling that the identity above partitions the k element subsets of $[n]$ into those which contain n and those which do not, we define:

$$f_{n,k}(x) = \begin{cases} f_{n-1,k}(x) & \text{for } x \leq \binom{n-1}{k} \\ \{n\} \cup f_{n-1,k-1}(x - \binom{n-1}{k}) & \text{for } \binom{n-1}{k} < x \end{cases}$$

1.7.1 Exercises

1. Using the algorithms specified in the section above, calculate the following explicitly:
   (a) The 25th sequence of length 3 from [3].

(b) The 25th sequence of length 3 from [4].

(c) The 24th permutation of [4].

(d) The 24th permutation of [5].

(e) The first 3 element subset of [10]

(f) The last 3 element subset of [10].

2. The *lexicographic ordering* of sequences, permutations, and subsets, is their ordering as they would occur in the dictionary (in the case of subsets we assume that the elements are listed in increasing order). That is, $1,5,7$ precedes $1,5,8$ and also $2,3,4$. Show that of the algorithms above, the bijection produces the sequences, and permutations, but not the subsets, in lexicographic order. How can the subsets algorithm be modified to obtain a lexicographic ordering?

3. (a) Describe an algorithm for producing a list of the k-permutations of a multiset in their lexicographic ordering. For example, the multiset $\{1,1,1,2,2,3\}$ has precisely 19, 3-permutations namely:

111	112	113	121	122
123	131	132	211	212
213	221	223	231	232
311	312	321	322	.

(b) Implement your algorithm.

4. (a) Describe an algorithm for calculating a bijection from

$$[n!/(n_1!n_2!...n_k!)] \quad \text{where } n = n_1 + n_2 + \cdots + n_k$$

to the permutations of the multiset:

$$\{\overbrace{1,1,\ldots 1}^{n_1},\overbrace{2,2,\ldots 2}^{n_2},\ldots,\overbrace{k,k,\ldots k}^{n_k}\}$$

(which should be considerably more efficient than listing all the permutations and selecting the appropriate one).

(b) Implement your algorithm.

5. A problem which is related to finding an explicit bijection is finding a method for randomly and uniformly selecting an object of a certain type. In fact, given a bijection we have such a method, by randomly and uniformly selecting an integer in an appropriate range and then applying the bijection. However, other methods may be more suitable

(mainly because they may require less computation). For example, the following algorithm is supposed to select a k-element subset uniformly from n. We presume that `Rand` returns a uniformly distributed random real in the range $[0, 1)$:

$$\begin{aligned}\texttt{RandomSubset}[k,n] = \textbf{If } &(\texttt{Rand} < k/n)\\ &\quad \{n\} \cup \texttt{RandomSubset}[k-1, n-1]\\ &\textbf{Else}\\ &\quad \texttt{RandomSubset}[k, n-1]\\ &\textbf{EndIf}\end{aligned}$$

(a) Does the algorithm work as claimed?

(b) Implement the algorithm and compare its behavior to using the explicit bijection for various values of k and n.

6. Find algorithms for randomly choosing a k-permutation from $[n]$, and for randomly choosing a k-multiset from $[n]$.

1.8 Gray Codes

There are of course many bijections possible between $\{0, 1, \ldots, 2^k - 1\}$ and the k-digit binary sequences (in fact there are $2^k!$ of them), only one of which was considered above. Suppose that you wish to transmit digital information (bit strings) using an analog transmission device (like a telephone, in which the intesity of the received signal can be measured). For simplicity, imagine that we wish to transmit 4 bit words, and will use a signal with 16 levels for the purpose. The most obvious approach would be to use a signal level equal to the value of a string considered as a binary number. However, detecting the precise level of the signal may be subject to some error, so the fact that 0111 and 1000 which differ in all four bits represent adjacent levels of signal intensity in the standard encoding is certainly undesirable. This is particularly significant in that there exist methods which can compensate for the corruption of a small number of bits in a signal, but which cannot deal with whole-scale changes of this type. Optimally we would like to have an encoding (i.e. bijection) $\mathcal{G}$ such that for two consecutive integers n and $n+1$, $\mathcal{G}(n)$ differs from $\mathcal{G}(n+1)$ in only a single bit. Such an encoding is indeed possible and Frank Gray of Bell Laboratories was awarded a patent for its discovery in 1943 (having applied for it in 1937). A further desirable feature of the original Gray code is that both the encoding and decoding process are very simple computationally.

We view a k-bit Gray code as a list of all the binary sequences of length k so that each element of the list differs from its predecessor in only one bit. For example, on the following page is a 4-bit Gray code $\mathcal{G}_4$ together with a list of the integers 0 through 15 in binary:

Can you determine how the 4-bit Gray code was constructed – can you construct a k-bit Gray code for each k? What about the encoding and decoding functions?

The main idea is to determine how to use a k-bit Gray code to generate a $(k+1)$-bit Gray code. Given a sequence $\mathcal{S} = s_1, s_2, \ldots, s_k$ of bit strings we let $\mathcal{S}^{op}$ denote the reverse of $\mathcal{S}$ namely the sequence $s_k, s_{k-1}, \ldots, s_2, s_1$. If $\mathcal{T} = t_1, t_2, \ldots, t_j$ is also a sequence of bit strings then we will define

$$\mathcal{S} \vee \mathcal{T} := s_1, s_2, \ldots, s_k, t_1, t_2, \ldots, t_j$$

Also given strings s and t we denote the string we get by concatenating s and t as $s^\frown t$. Finally, if $\mathcal{S}$ is a sequence, and s is a string, then $s^\frown \mathcal{S}$ will denote the sequence of strings obtained by concatenating s with each of the elements of $\mathcal{S}$. That is:

$$s^\frown \mathcal{S} = s^\frown s_1, s^\frown s_2, \ldots, s^\frown s_k.$$

n		$\mathcal{G}_4(n)$
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Proposition 13 *If $\mathcal{G}_k$ is a k-bit Gray code, then $(0^\frown \mathcal{G}_k) \vee (1^\frown \mathcal{G}_k^{op})$ is a $(k+1)$-bit Gray code.*

Proof: First observe that every $(k+1)$-bit binary string occurs exactly once in this list, since all the strings which begin with 0 occur in $0^\frown\mathcal{G}_k$ and all the strings which begin with 1 occur in $1^\frown\mathcal{G}_k^{op}$. Also, in the first half of the new list successive strings differ in only one bit, since their first bits are equal, and the remaining k bits are from successive strings in $\mathcal{G}_k$. The same applies in the second half of the list, since the reverse of $\mathcal{G}_k$ is clearly also a k-bit Gray code. Finally, the last element of the first half differs only in the first bit from the first element of the second half – since we have reversed $\mathcal{G}_k$ for the second half, so the final k bits of these two elements are the same. ∎

The Gray codes which are constructed according to this procedure have a further interesting property. Since $\mathcal{G}_{k+1}$ begins with $0^\frown\mathcal{G}_k$, the strings $\mathcal{G}_{k+1}(n)$ and $\mathcal{G}_k(n)$ represent the same integer if they are both defined. That is, we can represent all the Gray codes so constructed by a single function $\mathcal{G}$ from the non-negative integers to the non-negative integers whose value at an integer n is the common numerical value of all the strings $\mathcal{G}_k(n)$ for any k such that $n < 2^k$. The first sixteen values of this function can be read from the table above:

$$0, 1, 3, 2, 6, 7, 5, 4, 12, 13, 15, 14, 10, 11, 9, 8 \ldots$$

In the communication problem discussed at the beginning of this section we would like to be able to calculate both $\mathcal{G}(n)$ and $\mathcal{G}^{-1}(n)$ relatively easily. The second of these functions is needed in order to encode our input strings into intensity levels, and the first to decode the intensity levels back to strings at the other end. The form of these functions will be most easily determined if we think of them as functions from bit strings to bit strings. For convenience we do not specify the length of the strings exactly, but imagine that they have been padded to the left with a suitable number of 0's. To calculate $\mathcal{G}$ we need to determine the rule which takes us from the second column of the table to the third.

Proposition 14 *Let n be a non-negative integer and let the representation of n in base 2 be the bit string $\ldots b_k b_{k-1} \ldots b_2 b_1 b_0$. Then the base 2 representation of $\mathcal{G}(n)$ is the bit string $\ldots c_k c_{k-1} \ldots c_2 c_1 c_0$ where:*

$$c_j = b_{j+1} + b_j \pmod 2$$

for all j.

Proof: The result is clearly true if $n = 0$. Suppose now that m is a positive integer and that the result holds for all non-negative integers

which are smaller than m. Choose k such that $2^k \leq m < 2^{k+1}$. Thus the bit string representing m in base 2 has its leftmost 1 in the $(k+1)$st place. By the construction of $\mathcal{G}_{k+1}$,

$$\mathcal{G}(m) = 1^\frown \mathcal{G}(2^{k+1} - m - 1).$$

Observe that the $(k+1)$st digit of $\mathcal{G}(m)$ (namely 1) is the sum of the $(k+1)$st and the $(k+2)$nd digits of m. The number $(2^{k+1} - 1)$ has binary representation consisting of $k+1$ 1's so the binary representation of $m' = 2^{k+1} - m - 1$ is obtained by changing all the digits of m (from 1 to 0, or from 0 to 1). But this means, that except for the leftmost digit, the sum of successive digits of m' is the same as the sum of the corresponding digits of m modulo 2, and the leftmost (kth) digit is the sum of the $k+1$st digit of m (namely 1), and the kth digit of m. As the inductive hypothesis applies to m', and as we have just seen that adding successive digits of m' produces the same result as the corresponding additions for m, we have verified the claim for m, and hence proven the proposition by induction. ∎

Once we know the form of the function $\mathcal{G}$ (which in the communications examples enables us to decode intensities back to strings) it is a relatively simple matter to obtain the encoding function $\mathcal{G}^{-1}$. For if we have a bit string $\ldots c_k c_{k-1} \ldots c_2 c_1 c_0$ to encode, we want to find $\ldots b_k b_{k-1} \ldots b_2 b_1 b_0$ such that

$$c_j = b_{j+1} + b_j \pmod 2$$

for all j. Rewriting the above relation we get:

$$\begin{aligned} b_j &= c_j + b_{j+1} \pmod 2 \\ &= c_j + c_{j+1} + b_{j+2} \pmod 2 \\ &= c_j + c_{j+1} + c_{j+2} + b_{j+3} \pmod 2 \\ &\vdots \\ &= c_j + c_{j+1} + c_{j+2} + \cdots \pmod 2 \end{aligned}$$

The sum above only appears to be infinite, because we can stop adding up once we reach the leftmost 1 bit in $\ldots c_k c_{k-1} \ldots c_2 c_1 c_0$. Actually the first line of the above system tells us how to calculate $\mathcal{G}^{-1}$ in practice. We calculate the bits from left to right. The leftmost bit of $\mathcal{G}^{-1}(n)$ and n are the same, and thereafter the next bit is obtained by adding the last bit of $\mathcal{G}^{-1}(n)$ which had been calculated, to the bit of n which is in the position being filled. For example:

n	=	1	0	1	1	1	0	0	0	1	0
$\mathcal{G}^{-1}(n)$	=	1	1	0	1	0	0	0	0	1	1

Observe that each bit of $\mathcal{G}^{-1}(n)$ is the sum of the bit above it, and the bit immediately to its left.

1.8.1 Exercises

1. Calculate $\mathcal{G}(n)$ for each of the following n: 10, 53, 102, 3000, 10201.
2. Calculate $\mathcal{G}^{-1}(n)$ for each of the following n: 23, 34, 102, 651, 11210.
3. For which n is $\mathcal{G}(n)$ odd? For which n is $\mathcal{G}^{-1}(n)$ odd?
4. There are many other permutations of the 2^k bit strings of length k which are Gray codes. In fact, the exact number of k-bit Gray codes is unknown except for small values of k. Try to develop an algorithm which would in principle list all possible k-bit Gray codes for each k – you should be able to manage some improvement on simply testing each permutation of 2^k to determine whether or not it is a Gray code.

Chapter 2

Algebraic counting techniques

The title of this chapter is misleading. We intend to prove two algebraic theorems: the binomial theorem, and the principle of inclusion/exclusion, both of which have considerable application in enumerative problems. In particular, the basic idea underlying our proof of the binomial theorem leads to the entire subject of generating functions which is the heart of the link between combinatorics and algebra. We will only be able to explore a short distance along this path, but the reader who wishes to go further may consult some of the references at the end of the chapter.

2.1 The binomial theorem

Consider the following product (where $x_1, x_2, \ldots, x_n$ is a sequence of distinct variable symbols):

$$\begin{aligned} p_n &= \prod_{i=1}^{n}(1+x_i) \\ &= (1+x_1)(1+x_2)\ldots(1+x_n) \end{aligned}$$

When we expand p_n into a sum of *monomials* (terms which are constants times some product of x's), what will it look like? The first three cases may

give some information:

$$\begin{aligned} p_1 &= 1 + x_1 \\ p_2 &= 1 + x_1 + x_2 + x_1x_2 \\ p_3 &= 1 + x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 \end{aligned}$$

Note that p_1 contains 2 terms, p_2 contains 4 terms, and p_3 contains 8 terms, the same numbers as he number of subsets of a 1, 2 or 3 element set respectively. Nor does the correspondence stop here, in fact for each subset A of the set $\{x_1, x_2, x_3\}$ there is a monomial in p_3 formed by taking the product of those x's which belong to A (with the usual convention that an empty product equals 1). Thus, corresponding to the empty subset we have the monomial 1, to the subset $\{x_2, x_3\}$ the monomial x_2x_3, and to the whole set $\{x_1, x_2, x_3\}$ the monomial $x_1x_2x_3$. Further experimentation with larger values of n could only lead to the conclusion that this pattern persists (unless a mistake was made in evaluating p_n). In fact it is fairly clear why this pattern arises. Because

$$p_{k+1} = (1 + x_{k+1})p_k,$$

the monomials which occur in p_{k+1} are those which occur in p_k together with x_{k+1} times each monomial in p_k. This is very reminiscent of the way in which subsets of $[k+1]$ are generated from subsets of $[k]$. This idea forms the basis of an inductive proof of the following proposition.

Proposition 15 *For each positive integer n, the product p_n considered above, is equal to the sum of all the monomials formed from subsets A of $[n]$ by taking the product of the elements x_j for those $j \in A$. Formally:*

$$p_n = \sum_{A \subseteq [n]} \prod_{j \in A} x_j.$$

Proof: We have seen that the result holds for $n = 1$. Suppose that it holds for $n = m$, and consider

$$\begin{aligned} p_{m+1} &= \prod_{i=1}^{m+1} (1 + x_i) \\ &= p_m (1 + x_{m+1}) \\ &= \left(\sum_{A \subseteq [m]} \prod_{j \in A} x_j \right) (1 + x_{m+1}). \end{aligned}$$

In the final line we have used the hypothesis that the result holds for $n = m$. Now, by applying the distributive law, the right hand side of the final line can be written:

$$\left(\sum_{A\subseteq[m]}\prod_{j\in A}x_j\right)+x_{m+1}\left(\sum_{A\subseteq[m]}\prod_{j\in A}x_j\right)$$

The first term is already a sum of monomials, and the second becomes one when we bring x_{m+1} inside the summation:

$$\sum_{A\subseteq[m]}x_{m+1}\prod_{j\in A}x_j.$$

To each subset $B \subseteq [m+1]$ there now corresponds a monomial. If $m+1 \notin B$ then there is an appropriate monomial in the first summand above. If $m+1 \in B$ then, with $B' = B - \{m+1\}$, the monomial

$$\prod_{j\in B}x_j = x_{m+1}\prod_{j\in B'}x_j$$

occurs in the second summand. So p_{m+1} also has the form required by the proposition, and the result holds by induction. ∎

Something interesting happens when we replace the distinct variables

$$x_1, x_2, \ldots, x_n$$

by a single variable x. On the one hand, the product becomes $(1+x)^n$. On the other hand, a monomial,

$$\prod_{j\in A}x_j \quad \text{becomes} \quad x^{|A|}.$$

So from the proposition we obtain:

$$(1+x)^n = \sum_{A\subseteq[n]}x^{|A|}.$$

Now we can collect all the terms on the right which arise from sets of the same cardinality. Since for each $0 \leq k \leq n$ there are $\binom{n}{k}$ sets of size k we get:

Theorem 16 (The binomial theorem) *For every positive integer n,*

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

The following corollary is also useful:

Corollary 17 *For any a and b and any positive integer n,*

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

Proof: For $a = 0$ the result is trivial. If $a \neq 0$ then:

$$\begin{aligned}(a+b)^n &= a^n(1+(b/a))^n \\ &= a^n \sum_{k=0}^{n} \binom{n}{k} (b/a)^k \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.\end{aligned}$$

■

Actually, the corollary could also have been proven in a combinatorial way, by expanding $(a+b)^n$ into monomials, without taking into account the fact that a and b commute. Then each monomial is a sequence of n elements from $\{a, b\}$. The number of such monomials which reduce to $a^{n-k}b^k$ is just $\binom{n}{k}$ since that is the number of ways of choosing k places in the sequence for the b's.

The binomial theorem can be used to prove many identities. However, it is often the case that these identities can also be proved by combinatorial arguments, which may be more natural or illuminating. In the examples below we are sometimes guilty of using the theorem in this inappropriate fashion.

Example 27 *Prove that*

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

Solution: The left hand side is the coefficient of x^k in $(1+x)^{n+m}$. But $(1+x)^{n+m} = (1+x)^n(1+x)^m$. In general, the coefficient of x^k in the product of two polynomials is the sum over all $0 \leq j$ of the coefficient of x^j in the first and x^{k-j} in the second. This sum is precisely the right hand side above, and so we have proven the identity. ■

This is one of the cases of an inappropriate use of the theorem. We could simply have argued combinatorially that $\binom{n+m}{k}$ represents the number of k subsets of an $n+m$ element set. Each such subset contains a certain number, say j, of elements from among the first n elements of the set, which can be chosen in $\binom{n}{j}$ ways. The remaining $k-j$ elements come from the rest of the set, and can be chosen in $\binom{m}{k-j}$ ways. Adding up these distinct possibilities over all values of j gives the right hand side. In fact, this was given as an exercise in Chapter 1 section 4!

Example 28 *Prove that:*

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

Solution: The binomial theorem states:

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

If we differentiate both sides with respect to x we get:

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

Now if we substitute $x = 1$ we get:

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

as required. ∎

Again, there is a combinatorial proof. The left hand side counts the number of ways of choosing a specific element of an n element set and then a subset of the remainder. Think of the results as a "committee with chairman". If instead, we choose the whole committee first, and then a chairman from among them, this can be done in $k\binom{n}{k}$ ways for a k member committee. These results should be added over the possible values of k to give the right hand side.

Example 29 *Prove:*

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-2}{m-1} + \binom{n-3}{m-2} + \cdots + \binom{n-m}{1} + \binom{n-m-1}{0}.$$

Solution: This identity results from comparing the coefficients of x^m on the left and the right hand sides of the following identity:

$$\begin{aligned}(1+x)^n &= (1+x)^{n-1} + x(1+x)^{n-1} \\ &= (1+x)^{n-1} + x(1+x)^{n-2} + x^2(1+x)^{n-2} \\ &= (1+x)^{n-1} + x(1+x)^{n-2} + x^2(1+x)^{n-3} + x^3(1+x)^{n-3} \\ &\vdots \\ &= \sum_{j=0}^{n-1} x^j(1+x)^{n-1-j} + x^n\end{aligned}$$

■

The combinatorial proof is also not so easy to find. Consider an arbitrary m element subset of $[n]$. Let j be such that $n-j$ is the largest number which is not in the subset. The j largest elements of the subset are $\{n-j+1, n-j+2, \ldots, n\}$, and the remainder is an $m-j$ element subset of $[n-j-1]$. Adding up over these disjoint possibilities we get the required identity. As above, this was given as an exercise in Chapter 1 section 6.

Perhaps the easiest proof of this particular identity (which is suggested by the proof from the binomial theorem) is to begin from:

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

and to continue to split the rightmost term into two terms, until the identity is reached.

Example 30 *Prove that:*

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

Solution: Let ω be a complex cube root of 1. Since $\omega^3 - 1 = 0$,

$$(\omega - 1)(\omega^2 + \omega + 1) = 0.$$

But by our choice of ω we know that $\omega \neq 1$. Therefore,

$$\omega^2 + \omega + 1 = 0.$$

Now, from the binomial theorem:

$$(1+\omega)^{3n} = \sum_{k=0}^{3n} \binom{3n}{k} \omega^k.$$

Since $\omega^3 = 1$, we also have that

$$\begin{array}{ccccccc} \omega & = & \omega^4 & = & \omega^7 & = & \ldots \\ \omega^2 & = & \omega^5 & = & \omega^8 & = & \ldots \end{array}$$

Hence:

$$\begin{aligned} (1+\omega)^{3n} &= \sum_{k=0}^{n} \binom{3n}{3k} + \omega \sum_{k=1}^{n} \binom{3n}{3k-2} + \omega^2 \sum_{k=1}^{n} \binom{3n}{3k-1} \\ &= A + \omega B + \omega^2 C. \end{aligned}$$

Where A, B, and C are just convenient abbreviations for the three sums involved. A similar calculation shows that:

$$(1+\omega^2)^{3n} = A + \omega^2 B + \omega C$$

and finally:

$$2^{3n} = A + B + C.$$

But note that $1 + \omega = -\omega^2$, hence

$$(1+\omega)^{3n} = (-1)^{3n}\omega^{6n} = (-1)^{3n},$$

and similarly

$$(1+\omega^2)^{3n} = (-\omega)^{3n} = (-1)^{3n}.$$

Therefore we have the following system of equations:

$$\begin{array}{ccccccc} A & + & B & + & C & = & 2^{3n} \\ A & + & \omega B & + & \omega^2 C & = & (-1)^{3n} \\ A & + & \omega^2 B & + & \omega C & = & (-1)^{3n} \end{array}$$

If we add the three equations (and use $1 + \omega + \omega^2 = 0$) we get:

$$3A = 2^{3n} + 2(-1)^{3n}$$

as required. ∎

In fact the power of the binomial theorem extends far beyond the limited applications which we have seen here. First of all, if we define:

$$\binom{a}{k} = a(a-1)\ldots(a-k+1)/k!$$

for arbitrary a and integers $k \geq 0$, then the binomial theorem is valid for all exponents, not just positive integers. In the case where the exponent is not

an integer it gives a power series representation rather than a polynomial, and the power series converges for $|x| < 1$. For example:

$$\begin{aligned}(1+x)^{1/2} &= 1 + (1/2)x + \frac{(1/2)(-1/2)}{2}x^2 + \frac{(1/2)(-1/2)(-3/2)}{6}x^3 + \cdots \\ &= 1 + \frac{x}{2} - \frac{x^2}{8} + \frac{x^3}{16} - \frac{5x^4}{128} + \frac{7x^5}{256} + \cdots\end{aligned}$$

Even these power series have significant combinatorial interpretations. Just to give a single example: the coefficient of x^k in $(1-x)^{-n}$ counts the number of k multisets from an n element set. The interplay between counting and algebra which thus arises is the foundation of the subject of algebraic combinatorics.

We now state (and prove) a generalization of the binomial theorem. First we define a new symbol:

Definition 18 *Let n be a positive integer, and let $k_1, k_2, \ldots, k_m$ be a sequence of non-negative integers whose sum is n. Then:*

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \ldots k_m!}$$

is called a multinomial coefficient.

Theorem 19 (The multinomial theorem) *Let n be a positive integer. Then:*

$$(a_1 + a_2 + \cdots + a_m)^n = \sum \binom{n}{k_1, k_2, \ldots, k_m} a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}.$$

where the sum is taken over all sequences $k_1, k_2, \ldots, k_m$ of non-negative integers whose sum is n.

Proof: Either by a combinatorial argument as outlined following the proof of Corollary 17, or by repeated applications of this corollary and the associative law, we see that the coefficient of

$$a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$$

in

$$(a_1 + a_2 + \cdots + a_m)^n$$

is equal to:

$$\binom{n}{k_1}\binom{n-k_1}{k_2} \cdots \binom{n-k_1-k_2-\cdots k_{m-1}}{k_m},$$

the number of permutations of a multiset consisting of k_1 a_1's, k_2 a_2's and so on. But when this is expanded and simplified, it is easily seen to equal

$$\binom{n}{k_1, k_2, \ldots, k_m}$$

as required. ∎

2.1.1 Exercises

1. What is the coefficient of:
   (a) x^4 in $(1+x)^7$
   (b) x^3 in $(2+3x)^6$
   (c) x^2y^5 in $(ax+by)^7$
   (d) $xy^2w^3z^4$ in $(4x+3y+2z+w)^{10}$
2. Prove each of the following identities (practice using the binomial theorem, but think about other methods also).
   (a) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
   (b) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$
   (c) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \binom{n-3}{k-1} + \cdots$
   (d) Let $\mathbf{k} = k_1, k_2, \ldots, k_m$, and for $1 \leq j \leq m$ let $\hat{\mathbf{k}}_j$ be the sequence obtained by subtracting 1 from k_j and leaving the remainder of the sequence the same. That is:
   $$\hat{\mathbf{k}}_j = (k_1, k_2, \ldots, k_{j-1}, k_j - 1, k_{j+1}, \ldots k_m).$$
   If $k_1 + k_2 + \cdots + k_m = n$ then prove that:
   $$\binom{n}{\mathbf{k}} = \sum_{j=1}^{m} \binom{n-1}{\hat{\mathbf{k}}_j}.$$
3. Prove that the coefficient of x^k in:
   $$(1 + x + x^2 + x^3)^n$$
   is:
   $$\sum \binom{n}{j} \binom{n}{k-2j}.$$

4. (a) Prove the identity:

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

(b) Prove that for every polynomial $p(t)$ of degree d or less, there exists another polynomial $q(t)$, also of degree d or less such that the following is an identity:

$$q(n)2^{n-d} = \sum_{k=0}^{n} p(k)\binom{n}{k}.$$

(c) Prove, in fact, that there is a unique polynomial q with this property.

5. Using Taylor's theorem from calculus prove the generalization of the binomial theorem: for $|x| < 1$, and any real number a:

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

This result is due to Newton – and was one of the early triumphs of the development of calculus.

6. Is it true that for all $k \geq 0$, $\binom{1/2}{k}$ can be written as $m/2^n$ for some integers m and n? Show that:

$$\binom{1/2}{k} = \frac{(-1)^{k-1}}{2^{2k-1}k}\binom{2k-2}{k-1}.$$

What identity arises from the fact that:

$$(1+x)^{1/2}(1+x)^{1/2} = 1+x?$$

7. By considering the product:

$$\begin{aligned} q_n &= \frac{1}{1-x_1}\frac{1}{1-x_2}\cdots\frac{1}{1-x_n} \\ &= (1+x_1+x_1^2+\ldots)(1+x_2+x_2^2+\ldots)\cdots(1+x_n+x_n^2+\ldots) \end{aligned}$$

prove that the coefficient of x^k in $(1-x)^{-n}$ is equal to the number of solutions to the equation:

$$X_1 + X_2 + \cdots + X_n = k$$

with $X_1, X_2, \ldots, X_n$ non-negative integers.

2.2 The Inclusion/Exclusion Principle

A vexing question was left open when we introduced the rule of sum: what is the cardinality of the union of finite sets $A_1, A_2, \ldots, A_n$ when these sets are not disjoint? In some cases, it is possible to replace the sets by different finite sets which are disjoint but have the same union. Such adjustments are quite ad hoc and unsatisfactory in general, particularly when n is relatively large. Even in the case of two sets we saw that some information beyond the cardinalities of the individual sets was required. For two sets A_1 and A_2:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

So it appears that to determine the size of the union of finite sets requires some information about their intersection. Fortunately, in many combinatorial problems such information is available and for this reason an explicit formula, called the principle of inclusion/exclusion is often useful. We will now derive this formula and apply it to the following problems:

> How many permutations $a_1, a_2, \ldots, a_n$ of $[n]$ are there in which $a_i \neq i$ for each i?
>
> How many surjective functions are there from $[k]$ to $[n]$?

A permutation of the type mentioned above is called a "derangement". The problem is often stated in probabilistic terms as follows:

> Ten people arrive at a restaurant and check their coats. While they are eating, the hat check person partakes too liberally of the chef's cooking wine, so when they leave the coats are returned in random order. What is the probability that no person receives the correct coat?

The reader should think about trying to do these problems without proving something like the principle of inclusion/exclusion. We begin now towards a statement (and proof) of this principle by considering three sets:

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= |A_1 \cup (A_2 \cup A_3)| \\
&= |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)| \\
&= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| \\
&\quad - |(A_1 \cap A_2) \cup (A_1 \cap A_3)| \\
&= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| \\
&\quad - |A_1 \cap A_2| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|
\end{aligned}$$

Note the form of the final formula:

- Take the sum of the cardinalities of the individual sets.
- Subtract the sum of the cardinalities of all their two way intersections.
- Add the cardinality of all three way intersections.

We will see that this is a general pattern.

In the above computation we used only the facts that union and intersection are associative and commutative operations, that intersection distributes over union, and that the intersection of a family of sets (A_1, A_2, A_1, and A_3) is the same as the intersection of the distinct elements of the family (A_1, A_2, and A_3). In principle, these same rules could be applied inductively to provide a formula for the cardinality of the union of n sets, based on the rules for the earlier cases. For humans at least, such computations rapidly become tedious, although it is relatively easy to use symbolic manipulation programs to verify the formula for larger values of n.

To state the principle of inclusion/exclusion, we introduce some notation:

Let $A_1, A_2, \ldots, A_n$ be a sequence of finite sets. Let X be a non-empty subset of $[n]$. Set:

$$A_X = \bigcap_{x \in X} A_x$$

(so $A_{\{j\}} = A_j$ and $A_{[n]} = A_1 \cap A_2 \cap \cdots \cap A_n$).

Theorem 20 (Inclusion/Exclusion) *Let $A_1, A_2, \ldots, A_n$ be a sequence of finite sets. Then, with the notation defined above:*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \neq X \subseteq [n]} (-1)^{|X|-1} |A_X|.$$

Proof: We have seen above that the theorem is true for $n = 1$, 2, or 3. So we will prove the result by induction. Suppose that the result holds for $n = m$, and that $A_1, A_2, \ldots, A_{m+1}$ is a sequence of finite sets. Then:

$$\begin{aligned} &|A_1 \cup A_2 \cup \cdots \cup A_m \cup A_{m+1}| \\ &\quad = |A_1 \cup A_2 \cup \cdots \cup A_m| + |A_{m+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_m) \cap A_{m+1}| \end{aligned}$$

Consider each of the terms on the right hand side above in turn. From the inductive hypothesis, the first is:

$$\sum_{\emptyset \neq X \subseteq [m]} (-1)^{|X|-1} |A_X|.$$

The second is

$$(-1)^{(1-1)}A_{\{m+1\}}.$$

The third is:

$$|(A_{m+1} \cap A_1) \cup (A_{m+1} \cap A_2) \cup \cdots \cup (A_{m+1} \cap A_m)|$$

which by the inductive hypothesis (which applies to any sequence of sets) is equal to:

$$\sum_{\emptyset \neq X \subseteq [m]} (-1)^{|X|-1} |A_{m+1} \cap A_X|.$$

But setting $Y = X \cup \{m+1\}$ and bringing the minus sign inside the sum we get:

$$\begin{aligned} &|A_1 \cup A_2 \cup \cdots \cup A_{m+1}| \\ &= \sum_{\emptyset \neq X \subseteq [m]} (-1)^{|X|-1} |A_X| + (-1)^{(1-1)} A_{\{m+1\}} \\ &\quad + \sum_{Y} (-1)^{|Y|-1} |A_Y| \end{aligned}$$

In the first term we have all the non-empty subsets not containing $m+1$, and in the second and third terms all those which do contain $m+1$. So the above equals:

$$\sum_{\emptyset \neq X \subseteq [m+1]} (-1)^{|X|-1} |A_X|$$

as required, and by induction the result holds. ∎

In view of the importance of this theorem, and the opacity of the proof above, we offer another proof – which suffers only from the presupposition that the formula is known, whereas the proof above contains (in its inductive step) a recipe for determining the formula for $m+1$ sets from that for m. In the exercises we will offer a suggestion for a third proof. So again, we wish to prove:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \neq X \subseteq [n]} (-1)^{|X|-1} |A_X|.$$

Consider a single element $x \in A_1 \cup A_2 \cup \cdots \cup A_n$, and ask: how much does it contribute to the right hand side? If the formula is correct then this number should be 1, since we should count each element of the union of the sets exactly once. How can we determine this? Well, suppose that x belongs to exactly j of the sets $A_1, A_2, \ldots, A_n$. Then for each $k \leq j$, x belongs to

exactly $\binom{j}{k}$ of the sets A_X with $|X| = k$ (since the k sets must certainly be chosen from among those which have x as an element.) Moreover, for no $k > j$ does x belong to A_X for any X of cardinality k since at least one of the sets in such an intersection will not include x. So the total contribution to the right hand side which arises from x is:

$$\sum_{k=1}^{j}(-1)^{k-1}\binom{j}{k}.$$

But we have:

$$\begin{aligned} 0 &= (1-1)^j = 1 + \sum_{k=1}^{j}(-1)^k\binom{j}{k} \\ 1 &= -\sum_{k=1}^{j}(-1)^k\binom{j}{k} \\ 1 &= \sum_{k=1}^{j}(-1)^{k-1}\binom{j}{k} \end{aligned}$$

So, as required, each x in the union contributes 1 to the right hand side and the formula is correct.

Now we turn to the promised applications.

Example 31 *How many derangements are there of* $[n]$*?*

Solution: Can we solve this directly? Imagine trying to construct such a permutation. The first element must not be 1, so there are $n-1$ choices here. Now consider the second element. At first glance, it seems there are $n-2$ choices (anything but 2 or the number used in the first position), but in one case (if 2 was the number chosen for the first position), there are $n-1$ choices. Further pursuit of this line of reasoning will lead to an ever more complicated set of cases, and the chances of reaching the correct final answer are small (try it with $n = 5$).

In this, as in many other problems involving applications of the principle of inclusion/exclusion the first thing to do is to look at the complementary problem. If a permutation $a_1, a_2, \ldots, a_n$ is not a derangment, then for some i, $a_i = i$. That is, either the first element is a 1 or the second a 2 or ... or the nth is n. The presence of this "extended or" is a tip-off to the fact that we are looking at the union of a family of sets, and that the principle may

come into play. Since this is our first example we will proceed carefully and with great detail. Define the following sets (one for each j with $1 \leq j \leq n$):

$$A_j \quad = \quad \text{Those permutations of } [n] \text{ for which } a_j = j$$

Certainly we hope to determine the cardinality of the union of these sets. But the principle will not help us much if we cannot easily determine the cardinality of the intersection of some collection of them. So, given k of these sets $A_{j_1}, A_{j_2}, \ldots A_{j_k}$, set $X = \{j_1, j_2, \ldots, j_k\}$ and we seek to determine $|A_X|$. But A_X is precisely the set of permutations whose j_1st element is j_1, j_2nd element is j_2 ...That is, k of the values of the permutation are fixed, and the remaining $n-k$ are an arbitrary permutation of the remaining $n-k$ elements. So:

$$|A_X| = (n-k)!$$

Note that this depends only on $|X|$ and not on X – this often occurs in problems with a certain amount of symmetry like this, and as a result in the inclusion/exclusion formula, we may gather together the terms which arise from sets of the same size. Since there are $\binom{n}{k}$ terms arising from sets of size k, the number of non-derangements is:

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

So the number of derangements is:

$$\begin{aligned} n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} &= n! \sum_{k=0}^{n} \frac{(-1)^k}{(n-k)!} \\ &= n!(1/0! - 1/1! + 1/2! - 1/3! + 1/4! - \cdots) \end{aligned}$$

Notice that the sum in brackets converges (rapidly!) to e^{-1}. As a result it is possible to check that for all positive integers n, the number of derangements of n is the integer closest to $n!/e$.

In the case of the "hat check" problem of 10 hats, the probability of a derangement is the total number of derangements divided by 10! which is within 10^{-7} of $1/e$ (and more hats do not significantly effect the probability). ∎

Example 32 *How many solutions are there to the equation:*

$$X_1 + X_2 + X_3 + X_4 = 40$$

with each X_i a non-negative integer less than or equal to 15*?*

Solution: Were it not for the restriction that each $X_i \leq 15$ this would be the familiar problem of counting the number of 40-multisets of a 4 element set, and so the answer would be $\binom{43}{40}$. Among these solutions however, there are some which violate one or more of the upper constraints. Define:

$$A_i = \text{the set of solutions for which } X_i > 15$$

(note the possibility that other X's might also be too large.) The number of solutions which violate one or more of the constraints is the number of elements in $A_1 \cup A_2 \cup A_3 \cup A_4$. Consider A_1. Any solution in A_1 corresponds to a solution in non-negative integers to:

$$\begin{aligned}(16 + Y_1) + X_2 + X_3 + X_4 &= 40\\ Y_1 + X_2 + X_3 + X_4 &= 24\end{aligned}$$

So $|A_1| = \binom{27}{24}$. By symmetry:

$$|A_1| = |A_2| = |A_3| = |A_4| = \binom{27}{24}.$$

Now consider $A_1 \cap A_2$. Any solution in this set corresponds to a solution in non-negative integers to:

$$\begin{aligned}(16 + Y_1) + (16 + Y_2) + X_3 + X_4 &= 40\\ Y_1 + Y_2 + X_3 + X_4 &= 8.\end{aligned}$$

So $|A_1 \cap A_2| = \binom{11}{8}$. By symmetry:

$$|A_1 \cap A_2| = |A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_3| = |A_2 \cap A_4| = |A_3 \cap A_4| = \binom{11}{8}.$$

Clearly, any three or four way intersection is empty. Therefore:

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = 4\binom{27}{24} - 6\binom{11}{8}.$$

So the number of solutions which satisfy the constraints is:

$$\binom{43}{40} - 4\binom{27}{24} + 6\binom{11}{8}.$$

■

Example 33 *How many surjective functions are there from* $[k]$ *to* $[n]$*?*

Solution: Again we have a problem which does not yield readily to direct attack. Let us define $S(k,n)$ to be the number we seek (Warning! Not all authors agree with this notation and $S(k,n)$ may be used elsewhere to denote a related, but different, number. Always read the fine print!) If we consider the problem of constructing surjections, the key point arises when we come to the last element. If all of $[n]$ has been covered by the images of the previous elements, then we have n choices for its image. However, if there is an element which has been missed, then there is only one place to map k to which will yield a surjection. However, there are n possible elements which could have been missed. This at least yields a recurrence:

$$S(k,n) = \begin{cases} 0 & \text{for} \quad k < n \\ nS(k-1,n) + nS(k-1,n-1) & \text{otherwise} \end{cases}$$

The recurrence is useful for constructing a table of values, but tells us little about the general behavior of the function.

Again let us consider the complementary problem. A function which is not surjective misses one or more of the n elements of $[n]$. So we set:

$$A_i \quad = \quad \text{those sequences } a_1, a_2, \ldots, a_k \text{ which do not include } i$$

Given j such sets, the sequences which belong to their intersection omit j of n possible values. So there are $(n-j)^k$ such sequences. So the cardinality of the union of the A_j is:

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

which yields the formula:

$$\begin{aligned} S(k,n) &= n^k - \sum_{j=1}^{n} \binom{n}{j} (-1)^{j-1} (n-j)^k \\ &= \sum_{j=0}^{n} \binom{n}{j} (-1)^j (n-j)^k. \end{aligned}$$

Observing that $S(n,n) = n!$ yields the quite remarkable identity:

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

■

2.2.1 Exercises

1. A certain fraternity has 100 members. Of these, 85 play football, 80 play baseball, and 90 play basketball. What is the smallest possible number of them who play all three sports?

2. How many integral solutions to the equation:

$$X_1 + X_2 + X_3 + X_4 + X_5 = 20$$

are there with $0 \leq X_i \leq 5$ for $1 \leq i \leq 5$?

3. How many ways are there to distribute 6 identical balls into 4 boxes, if the first box can only hold one ball, the second two balls, the third three balls, and the fourth four balls?

4. How many positive integers less than 121 are primes? (Hint: any non-prime less than 121 has a prime factor of 2, 3, 5, or 7. By the way, 1 **is not** a prime.)

5. Thirteen cards are dealt off the top of a standard deck. As they are dealt the dealer says "two, three, four, ..., queen, king, ace". What is the probability that at some point during the deal, the card showing matched the one which the dealer said?

6. If eight dice are rolled, what is the probability that all six numbers will appear? What if 12 dice are used? Or 16?

7. How many "deranged sequences" of $[n]$ are there (where a sequence $a_1, a_2, \ldots, a_n$ is deranged if $a_i \neq i$ for every i)? Calculate this number using both the product rule and inclusion/exclusion. You should obtain an interesting identity.

8. How many permutations of $[n]$ do not contain consecutive digits of the form k, $k+1$ for any $1 \leq k \leq n$?

9. For a positive integer n, let $f(n)$ be the smallest value of k such that more than half of all the functions from $[k]$ to $[n]$ are surjective. How does $f(n)$ grow as a function of n?

10. Find a generalization of the principle of inclusion/exclusion which gives a formula for the number of elements x which occur in at least k of the sets $A_1, A_2, \ldots, A_n$ (inclusion/exclusion itself does this for $k = 1$).

11. Let $A_1, A_2, \ldots, A_n$ be finite sets and let U be a finite set which contains their union. Define the *characteristic function* of a subset $A \subseteq U$ to be the function:

$$\chi_A : U \to \mathbb{N}$$

defined by:

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in U - A. \end{cases}$$

(a) For any set $B \subseteq U$ show that:

$$|B| = \sum_{x \in U} \chi_B(x).$$

(b) For subsets $B_1, B_2, \ldots, B_n \subseteq U$ and $B = \bigcap_{i=1}^{n} B_i$ show that:

$$\chi_B = \prod_{i=1}^{n} \chi_{B_i}.$$

(c) Show that $\chi_{U-B} = 1 - \chi_B$.

(d) Use the above, and the fact that the intersection of the sets $U - A_i$ is U minus the union of the A_i to obtain:

$$1 - \chi_{A_1 \cup \cdots A_n} = \prod_{i=1}^{n} (1 - \chi_{A_i})$$

and expand the right hand side as in the proof of the binomial theorem, and then sum over $x \in U$ to obtain the principle of inclusion/exclusion.

That looks awfully complicated, but if you think about it, it is really the most natural of the three proofs (once you get used to thinking about the relationship between the "algebra of sets" and the arithmetic properties of their characteristic functions.)

2.3 An application

Consider the following problem:

For each non-negative integer k, find a formula for the following sum:

$$s_k(n) := 0^k + 1^k + 2^k + 3^k + \cdots + n^k = \sum_{j=0}^{n} j^k.$$

Such formulas are well-known for $k = 0, 1, 2, 3$ (we adopt the convention that $0^0 = 1$):

$$\begin{aligned} s_0(n) &= 1 + 1 + 1 + \cdots + 1 &&= n + 1 \\ s_1(n) &= 0 + 1 + 2 + 3 + \cdots + n &&= \tfrac{n(n+1)}{2} \\ s_2(n) &= 0^2 + 1^2 + 2^2 + 3^2 + \cdots + n^2 &&= \tfrac{n(n+1)(2n+1)}{6} \\ s_3(n) &= 0^3 + 1^3 + 2^3 + 3^3 + \cdots + n^3 &&= \tfrac{n^2(n+1)^2}{4} \end{aligned}$$

Furthermore, faced with a formula for the sum it is simple, albeit tedious, to verify it by induction. However, this does not help us to find formulas for the cases $n \geq 4$.

Here we will discuss three methods of solving this problem.

Method 1:

Based on the evidence of the first four cases we make the bold guess that the formula for k will be a polynomial in n of degree $k + 1$. That is, we guess:

$$s_k(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_k n^k + a_{k+1} n^{k+1}$$

For each particular value of n this gives us a system of linear equations for the unknown coefficients, $a_0, a_1, \cdots, a_{k+1}$. If we choose $k + 2$ different values for n we should be able to solve the resulting system of equations and obtain unique values for the a's.

As it happens, this works. For example, with $k = 4$ we get:

$$\begin{aligned} a_0 + a_1 + a_2 + a_3 + a_4 + a_5 &= 1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4 + 32a_5 &= 17 \\ a_0 + 3a_1 + 9a_2 + 27a_3 + 81a_4 + 243a_5 &= 98 \\ a_0 + 4a_1 + 16a_2 + 64a_3 + 256a_4 + 1024a_5 &= 354 \\ a_0 + 5a_1 + 25a_2 + 125a_3 + 625a_4 + 3125a_5 &= 979 \\ a_0 + 6a_1 + 36a_2 + 216a_3 + 1296a_4 + 7776a_5 &= 2275 \end{aligned}$$

This system has a unique solution:

$$a_0 = 0, \quad a_1 = -1/30 \quad a_2 = 0 \quad a_3 = 1/3 \quad a_4 = 1/2 \quad a_5 = 1/5.$$

But we still do not know for sure that this formula will work for all n so we would still have to check it by induction. Another problem with this method is that it presupposes that a polynomial of degree $k + 1$ will

give the sum. There is no real reason to expect this pattern to continue (but it does.) If we could prove that the pattern does continue, then the inductive checking of the formula would not be necessary since it is known that two polynomials of degree $k+1$ which agree at $k+2$ points must agree everywhere.

Although the solution of the system of linear equations would seem to be a difficult task, in fact this is quite easy (at least with mechanical assistance). All in all, if only there were some guarantee that a formula of this type exists this would not be a bad method.

Method 2:

Our second method is based on the observation:

$$\begin{aligned}(j+1)^{k+1} &= \sum_{i=0}^{k+1}\binom{k+1}{i}j^i \\ (j+1)^{k+1}-j^{k+1} &= \sum_{i=0}^{k}\binom{k+1}{i}j^i\end{aligned}$$

The first line is from the binomial theorem, and the second just rearranges it slightly. The value of this observation becomes apparent when we sum from 0 to n:

$$\begin{aligned}\sum_{j=0}^{n}((j+1)^{k+1}-j^{k+1}) &= \sum_{j=0}^{n}\sum_{i=0}^{k}\binom{k+1}{i}j^i \\ &= \sum_{i=0}^{k}\binom{k+1}{i}\sum_{j=0}^{n}j^i \\ &= \sum_{i=0}^{k}\binom{k+1}{i}s_i(n).\end{aligned}$$

Now on the left hand side we have:

$$\begin{aligned}&(1^{k+1}-0^{k+1})+(2^{k+1}-1^{k+1})+(3^{k+1}-2^{k+1}) \\ &\quad+\cdots+(n^{k+1}-(n-1)^{k+1})+((n+1)^{k+1}-n^{k+1}),\end{aligned}$$

and the negative part of eact term cancels the positive part of the preceding term (such a sum is said to "telescope".) So we get:

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

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

Hence:

$$s_k(n) = \frac{1}{k+1}\left((n+1)^{k+1} - \sum_{j=0}^{k-1} \binom{k+1}{j} s_j(n)\right).$$

This provides a method for calculating $s_k(n)$ and also we can see by induction that $s_k(n)$ will be a polynomial of degree $k+1$ in n with rational coefficients. However, to calculate s_k requires knowing the formulas for s_j for all $j < k$. So, in practice this may not be a tremendously practical method of evaluating s_k. It does justify the form of the formula which was assumed in Method 1, and hence validates that method.

Method 3:

Our final method really brings the heavy machinery to bear upon the problem. It is inspired by the observation that if only we were trying to calculate:

$$\binom{0}{j} + \binom{1}{j} + \binom{2}{j} + \cdots + \binom{n}{j}$$

instead of $s_k(n)$ then there would be no problem since we already know that the sum above equals:

$$\binom{n+1}{j+1}$$

(any $j+1$ element subset of $[n+1]$ has a largest element $m+1$ for some $0 \leq m \leq n$, and the rest of the subset is a j element subset of $[m]$. This identity is reappearing with tedious frequency.)

But this means that if we could write:

$$n^k = \sum_{j=1}^{k} a_j \binom{n}{j}$$

where $a_1, a_1, a_2, \ldots, a_k$ is a sequence of numbers which might depend on k but should not depend on n, then we could sum the left and the right hand sides separately. Perhaps a combinatorial argument should suggest why such a representation exists. The number n^k counts the number of functions from $[k]$ to $[n]$. Each such function has a range which may have j elements for any j between 1 and k. To specify a function with a j element range we should first specify which j elements are the range, which can be done in $\binom{n}{j}$ ways. Then we should choose a surjective function from $[k]$

to these j elements, which can be done in $S(k,j)$ ways (observe that this number does not depend on n.) Therefore, by rule of sum:

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

Hence:

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

This method requires us to calculate the coefficients $S(k,j)$ for which we could either use the exact formula from inclusion/exclusion, or the recurrence. It does not require knowledge of previous formulas for the sum of jth powers.

2.3.1 Exercises

1. Use each of the three methods to calculate $s_5(n)$. (You may not wish to use the first method in this case unless you have access to a suitable computer program for solving the resulting system of linear equations.)

2. Implement one or more of the methods in general. Which method works best for calculating a single function (like s_{20}?). Which works best for tabulating all the functions $s_1, s_2, \ldots, s_{20}$?

Chapter 3

Recurrences

3.1 What is a recurrence?

In many of the counting problems which we have considered there was a parameter n which was to be taken to be a positive integer. So in fact, in many cases we solved a whole family of counting problems giving a sequence of integers a_n, one for each positive integer n. In many cases we were able to find some relationship between a_n, and a_m for one or more $m < n$. Such a relationship is called a recurrence.

Definition 21 *A* recurrence *is a relationship among elements of a sequence a_n which determines the value of a_n in terms of one or more previous values a_k for $k < n$ in the sequence.*

Example 34 *Let a_n denote the number of binary sequences of length n. Then a_n satisfies the recurrence:*

$$a_n = 2a_{n-1}.$$

This trivial example none the less repays some further investigation. First of all, why is it true? Consider the set of all sequences of length n. These are divided into two types – those which end in 0 and those which end in 1. There are a_{n-1} of each type, since the final digit has no influence on the first $n-1$. Therefore $a_n = 2a_{n-1}$. Secondly, what good is it? Qualitatively it tells us how quickly the sequence a_n grows (it doubles at each step). But quantitatively it also determines the exact value of a_n for all n, once

we know the *base case* (which is the value of a_0, or of a_1 if you do not wish to consider sequences of length 0). For then, all the values of a_n are determined by the recurrence, and induction can be used to prove that in this case $a_n = 2^n$ for all n.

Henceforth, in questions involving sequences we will allow the empty sequence as a possibility.

Example 35 *Let b_n denote the number of binary sequences of length n which do not contain consecutive 1's. Then:*

$$\begin{aligned} b_n &= b_{n-1} + b_{n-2} \quad \textit{for} \quad n \geq 2, \\ b_1 &= 2, \\ b_0 &= 1. \end{aligned}$$

The analysis of the recurrence is much as above. Among the sequences of this type, there are those which end in 0 and those which end in 1. The sequences which end in 0 may have any of the b_{n-1} sequences of length $n-1$ as their initial $n-1$ digits. But those which end in 1 must end 01 or else they would contain consecutive 1's. But any of the b_{n-2} sequences of length $n-2$ may occur as their initial $n-2$ digits. If we add together the number of elements in these two cases, we obtain the recurrence. The base cases b_0 and b_1 are easily calculated explicitly. Note that we already worked this out in exercise 1.6.3.

Example 36 *Find a recurrence for the number of ways of expressing n as a sum of positive integers, where the order of the summation is considered to be important.*

The last phrase means that we are to consider $1+2+1$ and $2+1+1$ as different ways of representing 4. So, let s_n denote the number of ways of representing n. Any sum which equals n has a first term k with $1 \leq k \leq n$. The remainder of the sum is then just one of the s_{n-k} representations of $n-k$, except in the case where the first term is n, in which case there is nothing left to be added. Therefore:

$$s_n = s_{n-1} + s_{n-2} + \cdots + s_{n-k} + \cdots + s_2 + s_1 + 1.$$

There is another analysis which leads to a very different recurrence. Consider again the first term. It is either 1 or some number larger than 1. If it is 1, then the remainder of the sum is one of s_{n-1} representations of $n-1$.

If the number is larger than 1, then we can subtract 1 from it, and what remains is again one of the s_{n-1} representations of $n-1$. From this analysis we get:

$$s_n = s_{n-1} + s_{n-1} = 2s_{n-1}.$$

Which answer is right? They both are. Working with the first recurrence we get:

$$\begin{aligned} s_n &= s_{n-1} + s_{n-2} + \cdots + s_{n-k} + \cdots + s_2 + s_1 + 1 \\ &= s_{n-1} + (s_{n-2} + \cdots + s_{n-k} + \cdots + s_2 + s_1 + 1) \\ &= s_{n-1} + s_{n-1} = 2s_{n-1} \end{aligned}$$

So, in fact the two recurrences are the same. Obviously the second is easier to work with computationally. In fact, since $s_1 = 1$ it implies that $s_n = 2^{n-1}$ for all $n \geq 1$.

Example 37 *Consider all possible ways of parenthesizing the expression:*

$$x_1 x_2 x_3 \ldots x_n.$$

Let c_n denote the number of ways in which this is possible, which do not contain redundant parentheses, e.g.

$$((x_1 x_2))x_3.$$

Find a recurrence for c_n.

Solution: Any such parenthesization splits the expression into two parts. If the first part contains $x_1, x_2, \ldots, x_k$ then the second part consists of $x_{k+1}, x_{k+2}, \ldots, x_n$. As expressions in their own rights, the first part can be parenthesized in c_k ways, and the second part in c_{n-k} ways. Adding up over all the possible values of k gives:

$$\begin{aligned} c_n &= \sum_{k=1}^{n-1} c_k c_{n-k}, \\ c_1 &= 1. \end{aligned}$$

■

Note that recurrences such as the above may require the use of all the preceding values of the sequence, not just one or two.

3.1.1 Exercises

1. Find a recurrence for the number of ways of expressing n as a sum, where each term of the sum is 1, 2, or 3.

2. In example 36 we demonstrated that the number of ways to express n as a sum of positive integers is 2^{n-1}. Find a correspondence between the representations of n as such a sum and the subsets of $[n-1]$ which gives another proof of this result.

3. Show that the number of ways to express n as a sum of odd positive integers, denoted o_n satisfies the recurrence:

$$o_n = o_{n-1} + o_{n-3} + o_{n-5} + \cdots$$

with $o_0 = o_1 = 1$. Find a simpler form of the recurrence.

4. Find a recurrence for the number of n-sequences from $\{0, 1, 2\}$ in which every 2 is immediately preceded by a 1 and every 1 is immediately preceded by a 0.

5. Find a recurrence for the number of binary sequences which do not contain any subsequence of the form 000.

6. Show that the number of binary sequences which do not contain any sequence of the form 001 satisfies the recurrence:

$$a_n = 2a_{n-1} - a_{n-3}.$$

7. Show that the number of permutations of $[n]$ which do not contain a consecutive pair of the form k, $k+1$ satisfies the recurrence:

$$b_n = (n-1)b_{n-1} + (n-2)b_{n-2}.$$

3.2 Linear recurrences with constant coefficients

We now turn our attention to the question of finding a formula for a_n given initial values, and a recurrence. As the definition of a recurrence is so general, there is no real hope of solving this problem in full generality. We will, in this section at least, be content with finding the answer when the recurrence which a_n satisfies is of the form:

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

for a fixed positive integer k and fixed real numbers $c_1, c_2, \ldots, c_k$. We immediately rewrite this recurrence in the form:

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

In this form, it is called a *linear homogeneous recurrence with constant coefficients.* It is worth examining each of these words individually for a moment. The recurrence is called *linear* because each element of the sequence occurs individually, and not in a multiplicative combination with other elements, or with some other function applied. To illustrate by counterexample, neither of the following recurrences is linear:

$$\begin{aligned} a_n - a_{n-1}a_{n-2} - a_{n-3} &= 0 \\ a_n - \sin a_{n-1} + \cos a_{n-2} &= 0. \end{aligned}$$

The first is not linear because of the product term, and the second because other functions are applied to previous values of the sequence. The fact that the recurrence is *homogeneous* just means that the right hand side is 0 (this terminology is also used for other types of equations.) Finally, the recurrence is said to have *constant coefficients*, because it does!

Now, what can we do with this? The simplest case is when $k = 1$:

$$a_n - c_1 a_{n-1} = 0.$$

In this case, it is very easy to check by induction that:

$$a_n = (c_1)^n a_0$$

for all $n \geq 0$, so once we know the initial value of a_0 we have our formula. But what should we do when $k > 1$? One approach is to search for two things:

- a family of specific solutions, and
- some method of putting them together so that any family of initial conditions can be matched.

Before we embark on the first task, we had better see that we have some hope of carrying out the second, or we may be stuck with a bunch of particular solutions, and without a general answer. Fortunately, we have:

Theorem 22 (The superposition principle) *Suppose that*

$$a_1, a_2, \ldots, a_n, \ldots$$

and

$$b_1, b_2, \ldots, b_n, \ldots$$

are two sequences which satisfy the same homogeneous linear recurrence with constant coefficients:

$$x_n - c_1 x_{n-1} - \cdots - c_k x_{n-k} = 0.$$

Then for any real numbers r and s, the sequence defined by:

$$d_n = ra_n + sb_n$$

is also a solution to the same recurrrence.

Proof: The proof is a simple matter of calculation:

$$\begin{aligned} d_n - c_1 d_{n-1} - \cdots - c_k d_{n-k} &= (ra_n + sb_n) - c_1(ra_{n-1} + sb_{n-1}) - \\ &\quad \cdots - c_k(ra_{n-k} + sb_{n-k}) \\ &= r(a_n - c_1 a_{n-1} - \cdots - c_k a_{n-k}) \\ &\quad + s(b_n - c_1 b_{n-1} - \cdots - c_k b_{n-k}) \\ &= 0. \end{aligned}$$

■

By induction it is clear that for any finite set of solutions, any linear combination of them is still a solution to the same recurrence. Conversely, it is also clear that given any two solutions which satisfy the same initial conditions:

$$a_0 = b_0, a_1 = b_1, \ldots, a_{k-1} = b_{k-1},$$

then $a_n = b_n$ for all n. So to find a complete solution to the linear recurrence it suffices to produce sufficiently many individual solutions which can be combined to match any particular set of initial conditions.

Our search for specific solutions is motivated by the form of the solution when $k = 1$. In that case, each solution was an exponential one. It seems reasonable to ask which exponential functions are solutions to the more general recurrence.

Proposition 23 *Let the homogeneous linear recurrence with constant coefficients:*

$$x_n - c_1 x_{n-1} - \cdots - c_k x_{n-k} = 0$$

be given. For a constant λ, the sequence $a_n = \lambda^n$ is a solution to this recurrence if and only if:

$$\lambda^k - c_1 \lambda^{k-1} - \cdots - c_{k-1}\lambda - c_k = 0,$$

that is, if and only if λ is a root of the polynomial:

$$t^k - c_1 t^{k-1} - \cdots - c_{k-1} t - c_k = 0.$$

Proof: First suppose that $a_n = \lambda^n$ is a solution to the recurrence. Then evaluating the recurrence at a_k gives:

$$\lambda^k - c_1 \lambda^{k-1} - \cdots - c_{k-1} \lambda - c_k = 0.$$

Conversely, if λ is a root of this polynomial, and $a_n = \lambda^n$ then:

$$\begin{aligned} a_n - c_1 a_{n-1} - \cdots - c_k a_{n-k} &= \lambda^n - c_1 \lambda^{n-1} - \cdots - c_k \lambda^{n-k} \\ &= \lambda^{n-k}(\lambda^k - c_1 \lambda^{k-1} - \cdots - c_{k-1} \lambda - c_k) \\ &= 0. \end{aligned}$$

So in this case a_n is a solution to the recurrence. ∎

The polynomial

$$t^k - c_1 t^{k-1} - \cdots - c_{k-1} t - c_k = 0.$$

is called the *associated* or *characteristic* polynomial of the recurrence. Putting together the result above with the superposition principle we see that if $\lambda_1, \lambda_2, \ldots, \lambda_j$ are distinct roots of the characteristic polynomial, and $r_1, r_2, \ldots, r_j$ are real numbers, then any sequence of the form:

$$a_n = r_1 \lambda_1^n + r_2 \lambda_2^n + \cdots + r_j \lambda_j^n$$

is a solution of the recurrence. If the polynomial has k distinct roots, then it will be possible to match any initial conditions with such a solution, and hence this is the most general solution. After we look at some examples, we will examine the case where not all the roots of the equation are distinct.

Example 38 *Find the most general solution to the recurrence,*

$$x_n - 5x_{n-1} + 6x_{n-2} = 0$$

and use it to find a specific solution a_n with:

$$a_0 = 0, \text{ and } a_1 = 1.$$

Solution: The characteristic polynomial is:

$$t^2 - 5t + 6 = 0$$

which has roots $t = 2$ and $t = 3$. Therefore, the most general solution to the recurrence is:

$$a_n = r_1 2^n + r_2 3^n$$

for some real numbers r_1 and r_2. To match the specified initial conditions, we seek to find r_1 and r_2 such that:

$$\begin{aligned} r_1 + r_2 &= 0, \\ 2r_1 + 3r_2 &= 1. \end{aligned}$$

It is readily seen that $r_1 = -1$, $r_2 = 1$ is a solution to this system, so the particular solution to the recurrence which we seek is:

$$a_n = -2^n + 3^n.$$

■

Example 39 *Find a formula for the Fibonacci numbers:*

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ f_1 &= 1 \\ f_0 &= 0. \end{aligned}$$

Solution: The characteristic polynomial is:

$$t^2 - t - 1 = 0.$$

and its roots are:

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

To match the initial conditions we seek constants r_1 and r_2 such that:

$$\begin{aligned} r_1 + r_2 &= 0 \\ r_1\alpha + r_2\beta &= 1. \end{aligned}$$

It follows that:

$$r_1 = \frac{1}{\alpha - \beta} = 1/\sqrt{5}$$

and $r_2 = -r_1$. Therefore:

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

Notice that since $|\beta| < 1$, that for large n, f_n is very well approximated by the first term in the equation above. ∎

In the case where the characteristic equation has one or more repeated roots, the method which we have given will not provide enough solutions to match all possible initial conditions. However, in this case the following result (which we will not prove here, but which is fairly easy to check, and in any case can be derived quite easily from the results in the next section) provides the additional solutions which are required:

Proposition 24 *Suppose that $(t-\lambda)^j$ is a factor of the characteristic equation of a linear homogeneous recurrence with constant coefficients. Then for each integer i with $0 \leq i < j$ the sequence:*

$$a_n = n^i \lambda^n$$

is a solution of the recurrence.

Example 40 *Find a solution of the recurrence:*

$$a_n - 6a_{n-1} + 12a_{n-2} - 8a_{n-3} = 0$$

which satisfies $a_0 = 1$, $a_1 = 6$, $a_2 = 28$.

Solution: The characteristic polynomial:

$$t^3 - 6t^2 + 12t - 8 = (t-2)^3.$$

From the result above, $a_n = r_1 2^n + r_2 n 2^n + r_3 n^2 2^n$ is the general solution, and so we must solve the system of equations:

$$\begin{aligned} r_1 &= 1 \\ 2r_1 + 2r_2 + 2r_3 &= 6 \\ 4r_1 + 8r_2 + 16r_3 &= 28 \end{aligned}$$

The solution is $r_1 = r_2 = r_3 = 1$, and so the required sequence is:

$$a_n = (1 + n + n^2)2^n.$$

∎

We can also handle some cases of non-homogeneous recurrences. Namely, if we have a non-homogeneous linear recurrence with constant coefficients:

$$x_n - c_1 x_{n-1} - \cdots - c_k x_{n-k} = f(n),$$

then the difference between any two sequences which satisfy this recurrence is a sequence which satisfies the homogeneous recurrence:

$$x_n - c_1 x_{n-1} - \cdots - c_k x_{n-k} = 0.$$

Hence, the general solution of the non-homogeneous recurrence is the sum of any specific solution, and a general solution to the homogeneous recurrence. A specific solution can often be found by trying something of the same form as the right hand side.

Example 41 *Find the general solution of the recurrence:*

$$a_n - 2a_{n-1} = n^2,$$

and a specific solution with $a_1 = 1$.

Solution: The homogeneous equation has general solution $a_n = c2^n$. To handle the inhomogeneous part we look for a solution of the form $An^2 + Bn + C$. If this is a solution then:

$$\begin{array}{lcl} An^2 + B^n + C - 2(A(n-1)^2 + B(n-1) + C) & = & n^2 \\ (-A)n^2 + (4A - B)n + (-2A + 2B - C) & = & 1n^2 + 0n + 0 \end{array}$$

Since this should hold for every n, the coefficients of each term on either side must be the same. So $A = -1$, $B = -4$, and $C = -6$. So a particular solution to the recurrence is:

$$a_n = -n^2 - 4n - 6$$

and the general solution is:

$$a_n = -n^2 - 4n - 6 + c\,2^n.$$

To get $a_1 = 1$ requires $c = 4$. ∎

Example 42 *Find the general solution to:*

$$x_n - 3x_{n-1} + 2x_{n-2} = 3^n.$$

Find also a specific solution with $a_0 = a_1 = 1$.

Solution: The homogeneous part has associated polynomial $t^2 - 3t + 2 = 0$ with roots $t = 2$ and $t = 1$. So the general solution of the homogeneous part is:

$$a_n = r_1\,2^n + r_2\,1^n.$$

We will try $a_n = A\,3^n$ as a solution to the inhomogeneous equation. This yields:

$$A\,3^n - 3A\,3^{n-1} + 2A\,3^{n-2} = 3^n$$

which holds, provided that $2A = 9$, or $A = 9/2$. So the general solution of the recurrence is:

$$a_n = (9/2)\,3^n + r_1\,2^n + r_2\,1^n.$$

To fond the specific solution we need to find r_1 and r_2 such that:

$$\begin{aligned} 1 &= 9/2 + r_1 + r_2 \\ 1 &= 27/2 + 2r_1 + r_2 \end{aligned}$$

The solution to this is $r_1 = -9$, $r_2 = 11/2$. So the particular solution satisfying $a_1 = a_2 = 1$ is:

$$a_n = (9/2)\,3^n - (9)\,2^n + 11/2.$$

■

3.2.1 Exercises

1. Solve the following recurrences in general, and subject to the stated initial conditions:

   (a) $a_n - 3a_{n-1} + 2a_{n-2} = 0$ with $a_0 = 3$, $a_1 = 4$.

   (b) $a_n - 9a_{n-1} + 27a_{n-2} - 27a_{n-3} = 0$ with $a_0 = 1$, $a_1 = 3$, $a_2 = 27$.

   (c) $a_n - 2a_{n-2} + a_{n-4} = 0$ with $a_0 = 2$, $a_1 = 1$, $a_2 = 8$, $a_3 = 3$.

2. Solve each of the above if the right hand side is changed to $2n+1$ or 2^n (if 2^n is a solution of the homogeneous case, try a solution like $An2^n$ for the inhomogeneous case. A similar trick, like using a quadratic rather than a linear trial solution may also be required for the first type.)

3. Consider the recurrence:

$$a_n - a_{n-2} - a_{n-3} = 0$$

   (a) Show that the characteristic equation has two complex roots, but that the absolute value of these complex roots are both less than 1. (The absolute value of a complex number $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}$).

(b) Show that the real root ρ of the characteristic equation is approximately 1.3247.

(c) Show that for any real initial conditions a_0, a_1 and a_2, that for some real constant c,

$$\lim_{n\to\infty} |a_n - c\rho^n| = 0.$$

4. Use recurrences to find the formula for the sum of a geometric sequence:

$$a_n = 1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1}.$$

(either use $a_n - a_{n-1} = \lambda^{n-1}$ or $a_n - \lambda a_{n-1} = 1$.)

5. In the exercise for the previous section it was determined that the number of binary sequences not containing a subsequence of the form 001 satisfies the recurrence:

$$a_n - 2a_{n-1} + a_{n-3} = 0.$$

Find an exact formula for the number of such sequences.

6. Let a_n be a sequence which satisfies a linear homogeneous recurrence with constant coefficients whose characteristic equation is:

$$p(t) = 0.$$

Let $b_n = \sum_{k=0}^{n} a_k$. Prove that b_n satisfies a linear homogeneous recurrence with constant coefficients whose characteristic equation is:

$$(t-1)p(t) = 0.$$

3.3 Generating Functions

In this section we discuss a very general method for working with many different types of recurrences. We cannot do more than touch on the many problems which can be solved using this method, but we invite the interested reader to explore the subject further.

The basic idea is as follows: to any sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ we associate a power series, called the *generating function* for the sequence:

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots = \sum_{k=0}^{\infty} a_k t^k.$$

The parameter t should be viewed as a formal placeholder, which is really not doing anything other than separating the terms so that we can read off the values of our original sequence. However, information about the sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ may be reflected in algebraic properties of the "function" $f(t)$. In turn, such information may lead to a simple formula for the coefficients.

What algebraic operations can be performed on generating functions? Certainly they can be added and subtracted, multiplied by constants, powers of t or other generating functions. Moreover, they can be integrated or differentiated. In the table below we summarize the rules that go with these operations. It is convenient in many cases to adopt the convention that in a summation, any reference to a_k for $k < 0$ is to be taken to be 0.

Below:

$$\begin{aligned} f(t) &= \sum_{k=0}^{\infty} a_k t^k, \\ g(t) &= \sum_{k=0}^{\infty} b_k t^k. \end{aligned}$$

and c and d stand for real numbers, and n is a positive integer.

$$\begin{array}{lcl} cf(t) + dg(t) & = & \sum_{k=0}^{\infty} (ca_k + db_k) t^k \\ t^n f(t) & = & \sum_{k=0}^{\infty} a_k t^{n+k} = \sum_{k=0}^{\infty} a_{k-n} t^k \\ f(t)g(t) & = & \sum_{k=0}^{\infty} (\sum_{j=0}^{k} a_j b_{k-j}) t^k \\ f'(t) & = & \sum_{k=0}^{\infty} k a_k t^{k-1} = \sum_{k=0}^{\infty} (k+1) a_{k+1} t^k. \end{array}$$

In general, all the algebraic rules which one would expect to hold (associativity, commutativity, distributivity), together with the rules linking the algebraic operations to differentiation (sum and product) hold. Each of these should be formally verified, a task which we leave to the reader who has too much time on his/her hands.

Two very important power series which one needs to know in order to get anywhere at all are the Taylor series for $1/(1-x)$ and $1/(1+x)$. These are:

$$\begin{aligned} \frac{1}{1-x} &= 1 + x + x^2 + x^3 + \cdots + x^n + \cdots \\ \frac{1}{1+x} &= 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + \cdots \end{aligned}$$

(of course the second is easily derivable from the first by substitution.) These are often used with other things substituted for x. In the next example for instance we use the subsitution of $2t$ for x.

Now we turn to applications, beginning with a rather simple example.

Example 43 *Solve the recurrence* $a_n = 2a_{n-1}$.

Solution: Consider the associated generating function:

$$f(t) = \sum_{k=0}^{\infty} a_k t^k.$$

If $a_n = 2a_{n-1}$ for all n then:

$$\begin{aligned} f(t) - 2tf(t) &= \sum_{k=0}^{\infty} a_k t^k - \sum_{k=0}^{\infty} 2a_k t^{k+1} \\ &= a_0 + \sum_{k=1}^{\infty} (a_k - 2a_{k-1}) t^k \\ &= a_0. \end{aligned}$$

Hence:

$$(1 - 2t)f(t) = a_0$$

so

$$\begin{aligned} f(t) &= \frac{a_0}{1 - 2t} \\ &= a_0 \sum_{k=0}^{\infty} 2^k t^k \\ &= \sum_{k=0}^{\infty} (a_0 2^k) t^k \end{aligned}$$

By comparing coefficients we see that $a_k = a_0 2^k$ for all k ∎

In the above solution we made use of the following principle: if two power series are equal, then all their coefficients must be equal. Since we deal with power series primarily as formal objects, we could simply state this as an axiom. However, some of the algebraic manipulations which we carry out on power series presuppose a more concrete interpretation (as actual functions, at least for values of t for which they converge), and in this context the result above should be proven. However, this requires some complex analysis to carry out, so it will have to be accepted on faith.

The fact that we can solve a simple recurrence like the above is perhaps not too impressive. However, we can use generating functions to solve any of the recurrences considered in the last section. We illustrate with a further example involving repeated roots:

Example 44 *Solve the recurrence:*

$$a_n - 4a_{n-1} + 4a_{n-2} = 0$$

subject to the initial conditions $a_0 = 1$, $a_1 = 6$.

Solution: Let

$$f(t) = \sum_{k=0}^{\infty} a_k t^k.$$

Then:

$$\begin{aligned} f(t) - 4tf(t) + 4t^2 f(t) &= a_0 + (a_1 - 4a_0)t + \sum_{k=2}^{\infty} (a_k - 4a_{k-1} + 4a_{k-2})t^k \\ &= 1 + 2t. \end{aligned}$$

Hence:

$$f(t) = \frac{1+2t}{1-4t+4t^2} = \frac{1+2t}{(1-2t)^2}.$$

Now:

$$\begin{aligned} \frac{1}{1-2t} &= \sum_{k=0}^{\infty} 2^k t^k \\ \frac{1}{(1-2t)^2} &= \sum_{k=0}^{\infty} (k+1)2^k t^k \end{aligned}$$

(the second from the binomial theorem, or differentiating the first. By partial fractions:

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

hence:

$$a_k = -2^k + 2(k+1)2^k = (1+2k)2^k.$$

■

As a final example we consider a highly non-linear recurrence.

Example 45 *Recall that* c_n*, the number of ways of parenthesizing a product of* n *terms satisfies the recurrence:*

$$c_n = \sum_{j=1}^{n-1} c_j c_{n-j},$$

and $c_1 = 1$*. Find a formula for* c_n*.*

Solution: Consider the power series:

$$g(t) = \sum_{k=1}^{\infty} c_k t^k.$$

Then:

$$g(t)g(t) = \sum_{k=2}^{\infty}(\sum_{j=1}^{k} c_j c_{k-j})t^k.$$

Hence:

$$g^2(t) = g(t) - c_1 t = g(t) - t,$$

or:

$$g^2(t) - g(t) + t = 0.$$

If we think of this as a quadratic for an unknown quantity g in terms of t we get:

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

Which sign should we take? The idea is to use the binomial theorem to expand $\sqrt{1-4t}$. The coefficients of g are all positive, and the coefficients of this expansion are all negative except for the first. So to get positive coefficients for g we should take the $-$ sign in the numerator. Therefore:

$$\begin{aligned} g(t) &= \frac{1 - \sum_{k=0}^{\infty}\binom{1/2}{k}(-4)^k t^k}{2} \\ &= \sum_{k=1}^{\infty}(-1/2)\binom{1/2}{k}(-1)^k 4^k t^k. \end{aligned}$$

In the exercises following the proof of the binomial theorem, you were asked to prove that:

$$\binom{1/2}{k} = \frac{(-1)^{k-1}}{2^{2k-1}k}\binom{2k-2}{k-1}.$$

Hence:

$$\begin{aligned} g(t) &= \sum_{k=1}^{\infty}(-1/2)\frac{(-1)^{k-1}}{2^{2k-1}k}\binom{2k-2}{k-1}(-1)^k 4^k t^k \\ &= \sum_{k=1}^{\infty}(1/k)\binom{2k-2}{k-1}t^k. \end{aligned}$$

So

$$c_n = (1/n)\binom{2n-2}{n-1}.$$

■

3.3.1 Exercises

1. Solve the linear recurrence $a_n - a_{n-1} - 2a_{n-2} = 0$, $a_0 = a_1 = 3$ using generating functions.

2. Solve the linear recurrence $a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0$, $a_0 = 2$, $a_1 = 2$, $a_2 = 4$ using generating functions.

3. If $f(t)$ is the generating function for the sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$, and $b_n = \sum_{k=0}^{n} a_k$ then what is the generating function:

$$g(t) = \sum_{k=0}^{\infty} b_k t^k$$

(the answer should be in terms of $f(t)$, t, explicit constants, and simple algebraic operations.)

4. What does the coefficient of x^n in the series representation of

$$(1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}$$

count?

5. Define a_n to be the sequence given by the rule "a_n equals the number of 1's in the binary representation of n." So $a_0 = 0$, $a_1 = 1$, $a_{12} = 2$, etc.

   (a) Show that a_n satisfies the following recurrence:

$$\begin{aligned} a_n &= \begin{cases} a_k & \text{if } n = 2k, \\ a_k + 1 & \text{if } n = 2k+1, \end{cases} \\ a_0 &= 0. \end{aligned}$$

   (b) Let $f(t)$ be the generating function for a_n. Show that:

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