Chapter V: Generating Functions and Fast Arithmetic

Many useful methods and theorems in mathematics result from looking at the same entity in more than one way. For example, a kth-degree polynomial can be defined by its coefficients, or by its value at $k+1$ points. Taking this a step further, a $(k+1)$-digit decimal number N can be described by its $k+1$ decimal digits. These digits are the coefficients of a k-degree polynomial, $p_N(x)$, that characterizes the number: the number is the value of the polynomial when $x = 10$. (E.g. $p_{593}(x) = 5x^2 + 9x + 3$.) The polynomial $p_N(x)$, and hence N, can be determined by the values that the polynomial takes on at any $k+1$ values of x. In this chapter we shall see that we can use such alternative characterizations of the same number to multiply numbers much more rapidly than can be done with the standard method. But first we look at recurrence relations.

1 Recurrence Relations

Generating functions provide an alternative way to look at sequences. Given a (finite or infinite) sequence of coefficients a_n, their *generating function* is

$$\sum_n a_n x^n.$$

We will see how relations among sequences sometimes translate into relations among generating functions that allow us to determine the generating function, and thus provide a simple formula for the original sequence.

1.1 Convolution

One reason for the usefulness of generating functions comes from the fact that many recurrence relations between combinatorial functions a_n, b_n, and c_n take the form

$$a_n = \sum_{k=0}^{n} b_k c_{n-k}.$$

We say that the sequence $a_0, a_1, a_2, ...$ is the *convolution* of the sequence $b_0, b_1, b_2, ...$ and the sequence $c_0, c_1, c_2, ...$

This is the discrete analogue of the notion of convolution that you may have seen in continuous applied mathematics:

$$f(x) = \int g(t)h(x-t)\ dt.$$

There, an important technique was to take the Laplace transform of the three functions f, g, and h, obtaining new functions F, G, and H which satisfy the much simpler relation $F(x) = G(x)H(x)$.

In the setting of discrete mathematics, the analogue of a Laplace transform is a generating function. If you haven't seen Laplace transforms, don't be frightened! Generating functions are in fact much simpler. The generating function for the sequence $a_0, a_1, a_2, ...$ is the power series

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

You should check for yourself that if $B(x)$ and $C(x)$ are defined in terms of the sequences $b_0, b_1, b_2, ...$ and $c_0, c_1, c_2, ...$ in a similar way, the coefficient of x^n in $B(x)C(x)$ is precisely the right-hand-side of the convolution equation. Hence we have $A(x) = B(x)C(x)$ — a very compact and tractable way of expressing the dependence of the a_n's on the b_n's and the c_n's. Moreover, it is frequently the case that the $A(x)$ associated with a sequence $a_0, a_1, a_2, ...$ is given by a very simple algebraic function of x; for instance, if the sequence is $a, ar, ar^2, ar^3, ...$, the generating function is just $a/(1-rx)$.

Before we study an application of generating functions to convolutive recurrence relations, let's try a simpler example that nonetheless shows how generating functions can make your life easier.

1.2 Fibonacci Numbers

These numbers are defined as follows: $f_{-1} = 0$, $f_0 = 1$, and for $j \geq 1$,

$$f_j = f_{j-1} + f_{j-2}. \tag{1}$$

One can easily compute f_j for reasonably small values of j. One discovers that the ratio f_{n+1}/f_n of successive f's approaches the limit $\tau = (1+\sqrt{5})/2$ which is called the *golden ratio*.

Our recursive definition for f tells us how to compute f_n, once we have computed f_{n-1} and f_{n-2}, which requires that we have computed f_{n-3}, f_{n-4}, etc. We will use a generating function to obtain an *explicit* formula for the nth Fibonacci number (i.e. a formula depending only on n and not on previous f's). When we introduce a generating function, $F(x)$, for the Fibonacci sequence, we find that the recurrence relation for the f's translates into an equation for $F(x)$ that we can easily solve. Once we have $F(x)$ expressed in terms of partial fractions we can make use of the geometric series formula to expand $F(x)$ in powers of x, thereby obtaining an explicit formula for the f's. The same approach can be used for *any* "linear recursion with constant coefficients," like (1).

First we define $F(x)$:

$$F(x) = \sum_{j=0}^{\infty} f_j x^j.$$

Substituting for f_j using the recursion, and noting the values of f_{-1} and f_0, we obtain:

$$\begin{aligned}
F(x) &= \sum_{j=0}^{\infty} f_j x^j \\
&= 1 + \sum_{j=1}^{\infty} f_{j-1} x^j + \sum_{j=1}^{\infty} f_{j-2} x^j \\
&= 1 + \sum_{j=0}^{\infty} f_j x^{j+1} + \sum_{j=0}^{\infty} f_j x^{j+2} \\
&= 1 + \left(\sum_{j=0}^{\infty} f_j x^j \right) \cdot x + \left(\sum_{j=0}^{\infty} f_j x^j \right) \cdot x^2 \\
&= 1 + xF(x) + x^2 F(x).
\end{aligned}$$

This solves to

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

The quadratic polynomial in the denominator of this equation has roots at $\alpha = 1/\tau = (-1+\sqrt{5})/2$ and $\beta = -\tau = (-1-\sqrt{5})/2$. We use partial fractions: since $\alpha - \beta = \sqrt{5}$,

$$\begin{aligned}
\frac{1}{1-x-x^2} &= \frac{1}{\sqrt{5}(\alpha - x)} - \frac{1}{\sqrt{5}(\beta - x)} \\
&= \frac{\alpha^{-1}}{\sqrt{5}(1 - x/\alpha)} - \frac{\beta^{-1}}{\sqrt{5}(1 - x/\beta)} \\
&= \frac{1}{\sqrt{5}} \left(\sum_{j=0}^{\infty} \frac{x^j}{\alpha^{j+1}} - \sum_{j=0}^{\infty} \frac{x^j}{\beta^{j+1}} \right).
\end{aligned}$$

Hence

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

Looking at just the above form, it is surprising that f_j will always be an integer, but the integrality of f_j is clear from our earlier, recursive definition. Moreover, the second term goes to zero exponentially fast as a function of j, so that the first term, which grows by a factor of τ each time j increases by 1, dominates almost completely. (The terms $\tau^7/\sqrt{5}$ and $\tau^8/\sqrt{5}$ are approximately 21.0095 and 33.9941.)

More generally, suppose we had a sequence $g_{-1}, g_0, g_1, \ldots$ satisfying $g_j = g_{j-1} + g_{j-2}$ for all $j \geq 1$. If we let $G(x) = \sum_{j=0}^{\infty} g_j x^j$ we find that

$$G(x) = \frac{g_0 + g_{-1}x}{1 - x - x^2}.$$

Using partial fractions, we can find constants A and B (depending on g_0 and g_{-1}) such that

$$\frac{g_0 + g_{-1}x}{1 - x - x^2} = \frac{A}{1 - x\tau} + \frac{B}{1 + x/\tau}.$$

Hence

$$G(x) = A \sum_{j=0}^{\infty} \tau^j x^j + B \sum_{j=0}^{\infty} (-1/\tau)^j x^j,$$

so that

$$g_j = A\tau^j + B(-1/\tau)^j.$$

Here we were able to derive explicit solutions for both $G(x)$ and g_j. We are not always so lucky.

1.3 Catalan Numbers

Now we will examine a problem in which generating functions make their full usefulness felt, via the convolution formula.

Consider a string containing n left and n right parentheses. We now ask: in how many ways can the string be ordered so that it is *well-formed* in that all parentheses close, using the usual rule for closing parentheses? The answer is called the nth *Catalan Number* which we will denote by c_n.

The rule for closing parentheses is: a left parenthesis followed immediately by a right parenthesis can be closed with the latter, and the resulting pair can then be ignored in closing among the rest of the parentheses. For example, $c_1 = 1$; of the two possible arrangements)(and () , only the latter is well-formed. Also $c_2 = 2$: (()) and ()() .

The Catalan numbers arise in several seemingly unrelated contexts. Suppose we start with $n + 2$ points connected to form a polygon. Then we draw chords joining pairs of points in such a way that no two chords cross and they divide the interior of the polygon into triangles. The number of ways to triangulate a polygon, which we denote by d_n, also turns out to be c_n. But before proving this, let us find a simple explicit formula for c_n, again by use of a generating function.

In the parentheses problem, if a string is well-formed, the first parenthesis must be a (. It must close with some) somewhere, say the $(j+1)$st) $(0 \le j \le n-1)$. Then the j left and j right parentheses that lie within this parenthesis pair must be well-formed; similarly the $2(n-j-1)$ parentheses that follow the $(j+1)$st) must be well-formed. Therefore c_n obeys the equation:

$$c_n = \sum_{j=0}^{n-1} c_j\, c_{n-1-j} \qquad \text{for } n > 0, \tag{3}$$

with $c_0 = 1$. Using this equation, we may successively calculate $c_2 = 2$, $c_3 = 5$, $c_4 = 14$, etc.

This equation says that the c_n's are a convolution of one another. Hence, let us define the generating function for these numbers, $C(x)$:

$$C(x) = \sum_{j=0}^{\infty} c_j x^j. \tag{4}$$

By multiplying the convolution equation above by x^n and summing over $n \ge 1$, we deduce that

$$C(x) - 1 = x \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} (c_j x^j) \cdot (c_{n-1-j} x^{n-1-j}) = xC(x)^2.$$

By the quadratic formula, this equation has the solution

$$C(x) = (1 - (1-4x)^{1/2})/(2x).$$

(It can be shown that the other solution to this quadratic, coming from the positive square root, is not a possible solution here because it has a $1/x$ term in it.)

The binomial theorem tells us the coefficient of x^n in this expression:

$$c_n = -C(1/2, n+1)(-4)^{n+1}/2.$$

This is our explicit formula. Here $C(a,b)$ is the generalized binomial coefficient, given by the formula $a_{(b)}/(b!)$ where $a_{(b)}$ is $a \cdot (a-1) \cdots (a-b+1)$. (Recall that the binomial theorem works for any power, integer or not, as it follows from the Taylor series formula $(1+x)^z = \sum z_{(n)} x^n/(n!) = \sum C(z,n) x^n$.)

There is an easier way to obtain the same formula. Since there are $C(2n, n)$ orderings of our parentheses all told, we can count those that are well-formed by counting those that aren't. Any ordering R of our $2n$ parentheses which isn't well-formed has at least one pair of parentheses which do not close (because they occur

Figure 1: A triangulation for $n+2=7$.

in the order) . . . (in R). Consider the last right parenthesis which fails to close in R, and define $s(R)$ to be the ordering of parentheses in which this parenthesis is switched to a left parenthesis but all other parentheses in $s(R)$ are exactly as they are in R. For example, if $R =$))()()((then $s(R) =$)(()()((.

Obviously $s(R)$ has $n+1$ ('s and $n-1$)'s. Furthermore, if we start with any sequence of $n+1$ ('s and $n-1$)'s, at least two left parentheses won't close and we can switch the first such parenthesis to a right parenthesis to obtain a sequence with an equal number of lefts and rights; this will take $s(R)$ back to R. The mapping R to $s(R)$ is therefore completely onto all the sequences of $n+1$ left and $n-1$ right parentheses. Thus the number that are not well-formed is $C(2n, n-1)$. Hence the number that are well-formed is

$$c_n = C(2n, n) - C(2n, n-1).$$

It is left as an exercise to show that this agrees with the above formula.

Now let us consider triangulations of a polygon by chords. We will deduce an identical convolution property for d_n.

Suppose we have $n+2$ vertices forming a convex polygon. Then the edge of the polygon joining vertex 1 to vertex $n+2$ must belong to a unique triangle in the triangulation, say with third vertex $j+2$ $(0 \leq j \leq n-1)$. Then the vertices 1 to $j+2$ form a triangulation among themselves within the part of the polygon cut by the chord $(1, j+2)$, which can be arranged in d_j ways, and the vertices from $j+2$ to $n+2$ form a triangulation on one side of the chord $(j+2, n+2)$, which can be done in d_{n-j-1} ways. (See Figure 1.) We again obtain the convolution recurrence:

$$d_n = \sum_{j=0}^{n-1} d_j \, d_{n-1-j} \qquad \text{for } n > 0,$$

and $d_0 = 1$, so we can conclude that $d_n = c_n$.

1.4 Renewal Processes

Let $E_1, E_2, \ldots$ be random events as in Chapter III. We say they form a *renewal sequence* or *renewal process* if, letting p_k denote the probability of the event E_k, it is the case for all j, k that the conditional probability $P(\, E_{k+j} \mid E_j \,)$ satisfies

$$P(\, E_{k+j} \mid E_j \,) = p_k = P(E_k).$$

For instance, suppose we have a sequence of bits $a_0, a_1, \ldots$ generated by repeatedly tossing an unbiased coin. If we let E_k be the event that after k steps, the last five bits seen $(a_{k-4}, a_{k-3}, a_{k-2}, a_{k-1}, a_k)$ are 0,0,0,0,1, respectively, then the events E_k form a renewal sequence. However, if we let E_k be the event that the last five bits seen were all 0's, then we do not obtain a renewal sequence. The significance of requiring that a_k is 1, rather than 0, is that it "resets the clock"; hence the term "renewal sequence". Sometimes we will refer to "the renewal event E," but this is just a handy way of speaking of the events E_1, E_2, ... in aggregate.

We address the question: what is the probability that the renewal event E occurs *for the first time* at the nth stage? That is, letting S denote the full sample space, what is the probability of the event

$$(S - E_1) \cap (S - E_2) \cap \cdots \cap (S - E_{n-1}) \cap E_n \ ?$$

We denote this probability by f_n. (Notice that the f's will sum to at most 1.)

We answer this question by defining a generating function, $G(x)$, for the probabilities p_n, and another one, $F(x)$, for the first-time probabilities f_n. We can in many situations solve for $G(x)$, and there is a general relation between $F(x)$ and $G(x)$, which together give us an expression for $F(x)$, which we can, with luck, expand to obtain the f's.

The generating functions are defined as follows:

$$G(x) = \sum_{n=1}^{\infty} p_n x^n \qquad \text{and} \qquad F(x) = \sum_{n=1}^{\infty} f_n x^n.$$

An event which occurs at the nth bit either happens for the first time, or it happened before and did so last at the jth bit. This statement translates to the recursion

$$p_n = f_n + \sum_{j=1}^{n-1} p_j f_{n-j},$$

which is again a convolution.

Multiplying this by x^n and summing over n yields

$$G(x) = F(x) + G(x)F(x).$$

which can be rearranged into either

$$F(x) = \frac{G(x)}{1 + G(x)}$$

or

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

Suppose the event E is that the previous five bits are 00001, and let us suppose that the bits are random and independent, with each bit having probability 1/2 of being a 0 or of being a 1. Then the probability of this event is 1/32 for all $n \geq 5$ and 0 for $n < 5$. Therefore

$$G(x) = x^5/32 + x^6/32 + \ldots = x^5/(32(1-x)),$$

and thus, from above,

$$F(x) = x^5/(32(1-x) + x^5).$$

We will not extract the f's from this expression for F here, but in many cases (especially where the denominator has low degree) one can use partial fractions again to do this, after extracting the roots of the denominator. (In our case, the denominator has degree 5, so we would have to extract the roots numerically. Each term in the partial fraction expression will decrease exponentially in n with the rate of decrease computable from the roots of the fifth-degree polynomial that appears in $F(x)$.)

Another interesting renewal event is making a new high score after n bits, where the score is the number of ones minus the number of zeroes. Another example is "breaking even after $2n$ bits" which means having the same number of zeroes as ones after the $2n$th bit. The probability of having this happen for the first time at n can be determined by following the plan above.

In general the sum of the f's is $F(1)$. This will be 1 if the event E has probability 1 of happening eventually. In that case, notice that $G(1)$ must be infinite. Conversely, if $G(1)$ is infinite then $F(1) = 1$. An interesting question often is: does E almost surely happen eventually, or is there a finite possibility of escaping it? If we use "breaking even after $2n$ steps" in the usual unbiased coin-toss situation as our event E, its probability is $C(2n, n)/2^{2n}$, which is of the order of $n^{-1/2}$. The sum of this over n diverges, which means that $G(1)$ is infinite in this case. Hence $F(1) = 1$.

The problem can be viewed as a one-dimensional random walk, in which moving forward and back each have probability 1/2. The divergence of $G(1)$ means that with probability 1 we will eventually get back to our starting point. For a random walk in 2 dimensions, in which one wanders in one of 4 directions, the probability of breaking even after $2n$ is on the order of n^{-1}, since we figure to have taken roughly n steps parallel to both axes, and get a factor of $n^{-1/2}$ from each axis. (This is only as a heuristic argument, but it can be shown that it gives the right answer, qualitatively.) The sum of n^{-1} for $G(1)$ still diverges; so again with probability 1 we return to the origin eventually. On the other hand, for a random walk in 3 dimensions, we similarly expect factors of $n^{-3/2}$ in $G(1)$, which gives rise to a convergent series, and hence implies that there is a finite probability of escaping and never returning to the origin for random walks in 3 dimensions.

1.5 Permutations without Fixed Points

There are $n!$ permutations (or orderings) of a set S of n symbols. By fixing an ordering of S, each permutation can be described by listing the positions of the first through the nth symbol. For example, the permutation $n, \ldots, 1$ reverses the order of all the symbols. A permutation is said to have a *fixed point* if some symbol is in the same position after the permutation that it was in before it. We want to know the number of permutations with no fixed point. Let $a_n n!$ be this number; then a_n gives the proportion of permutations with no fixed point ($0 \leq a_n \leq 1$).

If we count all pairs of the form (permutation p, set $A(p)$ of fixed points of p), we obviously get $n!$, since each permutation has exactly one set of fixed points. If we count such pairs by A's, we thus obtain that

$$n! = \sum_{A \subseteq S} (\# \text{ of permutations whose fixed point set is } A).$$

If p has A as its fixed point set, then p must be the identity permutation within A, and on $S - A$ it must be a permutation with no fixed points. If A has j elements, the number of such p is therefore $(n-j)!\, a_{n-j}$. For each j there are $C(n, j)$ possible A's each having this number of permutations, so that

$$n! = \sum_{j=0}^{n} a_{n-j}\, C(n, j)\, (n-j)! = n! \sum_{j=0}^{n} a_{n-j}/j!.$$

Multiplying this by $x^n/n!$ and summing over $n \geq 0$ we obtain:

$$\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} \sum_{j=0}^{n} a_{n-j} x^n/j! = \sum_{j=0}^{\infty} \sum_{n=j}^{\infty} (a_{n-j} x^{n-j})(x^j/j!).$$

If we introduce the generating function

$$A(x) = \sum_{n=0}^{\infty} a_n x^n,$$

then the preceding equation can be rewritten as

$$(1-x)^{-1} = A(x)e^x,$$

and thus

$$A(x) = (1-x)^{-1}e^{-x}.$$

¿From this we may deduce what a_n is: because of the nature of the geometric series here, every term in the series for e^{-x} up to the nth-order term will provide a contribution to the coefficient of x^n, and that contribution will be exactly what appears in the Taylor expansion of e^x evaluated at $x = -1$:

$$a_n = 1 - 1/1! + 1/2! - 1/3! + 1/4! - \ldots \pm 1/n!\ .$$

This is a very rapidly converging series, so that for n of any reasonable size, the proportion p_0 of permutations without a fixed point is close to $1/e$.

If we have n independent repetitions of a random event E which has probability p, we obtain a binomial distribution for the number of occurrences of E among these. When p is c/n for a constant c, this distribution approaches what is called a *Poisson Distribution*: the probability p_k of k occurrences approaches $e^{-c}c^k/k!$. Here, the event that j is a fixed point among all permutations has probability $1/n$ so that $c = 1$. It is not true that the occurrences of this event at different j are independent: if there is a fixed point at j, the probability of there being one at k is increased to $1/(n-1)$. However this dependence is sufficiently small that one still gets approximately a Poisson Distribution, for which we evaluated the p_0 value above.

Exercises.

1. The Shmiconacci Numbers obey $s_{-1} = 0$, $s_0 = 1$, and $s_j = s_{j-1} + 2s_{j-2}$ for $j \geq 1$. Find an explicit formula for them.

2. Show that the following three expressions are equal:
$C(2n, n) - C(2n, n-1)$, $C(2n, n)/(n+1)$, and $-C(1/2, n+1)(-4)^{n+1}/2$.

3. Let a_n denote the number of ways of tiling a 1-by-n rectangle with red 1-by-1 blocks, blue 1-by-1 blocks, and green 1-by-2 blocks, so that $a_1 = 2$, $a_2 = 5$, etc.
(a) Find a recurrence relation for the numbers a_n. Check that your recurrence relation is correct by verifying that it gives the correct values of a_3 and a_4.
(b) Express this recurrence relation as an algebraic property of the generating function $A(x) = \sum_{n=0}^{\infty} a_n x^n$.
(c) Use this algebraic property to solve for $A(x)$. (Note: "solving" for $A(x)$ means finding a formula like $A(x) = 1/(1-x-x^2)$ or $A(x) = (1-\sqrt{1-4x})/2x$.)
(d) Find a formula for a_n.

4. Say that a sequence of)'s, ('s, and X's is *good* if removing the X's yields a well-formed string of parentheses. Let s_n be the number of good strings of length n. Thus for example $s_3 = 4$, since ()X, (X), X(), and XXX are the good strings of length three.
(a) Find a recurrence relation for the numbers s_n.
(b) Express this recurrence relation as an algebraic property of the generating function $S(x) = \sum_{n=0}^{\infty} s_n x^n$.
(c) Use this algebraic property to solve for $S(x)$.

5. (hard) Suppose we have n left parentheses and $2n$ right parentheses, and each left must close with two rights, under the rule that one can close a left with two adjacent rights, and then ignore the presence of all three in closing the rest. How many different ways of doing this are there?

6. For $n \geq 0$, let $A_n = \sum_{k=0}^{n} F_k 2^{n-k}$, where F_k is the kth Fibonacci number (with $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, et cetera). Thus the sequence $A_0, A_1, A_2, \ldots$ goes 1, 3, 8, 19, 43, ... Express $\sum_{n=0}^{\infty} A_n x^n$ as a rational function of x. (Hint: the sequence 1, 3, 8, 19, 43, ... is the convolution of the sequences 1, 1, 2, 3, 5, ... and 1, 2, 4, 8, 16, ...) Do not try to find a closed-form formula for A_n.

2 Resistance of Networks

For our next application of generating functions we look at the problem of finding the steady state resistance of a complicated electrical network.

Current flow in circuits is governed by Kirkhoff's Laws which lead to certain matrix equations that can be solved for the resistance of the network between probes placed at any two points in it. By use of generating functions, we will prove the *matrix-tree theorem* which relates this resistance to a ratio of two sums over trees in the network. We shall see that this result allows us to read off the resistance of a whole range of peculiar networks with no work at all. You will be able to amaze yourself and your friends with your prowess in answering such questions.

First, however, you may want to brush up on some linear algebra. In particular, you might want to remind yourself about basic properties of the determinant of a matrix, so that in particular, you see that an n-by-n matrix of the form

$$M = \left(\begin{array}{c|c} 1 & * \cdots * \\ \hline 0 & \\ \vdots & M' \\ 0 & \end{array}\right).$$

has the same determinant as its $n-1$-by-$n-1$ sub-matrix M'.

2.1 Circuits

We consider networks consisting of nodes $1, 2, \ldots, n$ with various connections between them, the connection between node i and j having resistance R_{ij}. If i and j are not connected, set $R_{ij} = \infty$. Say we probe the resistance between nodes 1 and n.

Ohm's law tells us that there is a potential, V_j, at node j, and a current I_{ij} from node i to node j with $I_{ij} = (V_i - V_j)/R_{ij}$. Kirkhoff's laws tell us that the sum of the currents into every node (except the two terminals where our probes are) is the same as the sum of currents going out. Since we count current going out as negative current coming in, this says that for $i = 2$ to $n-1$ we have

$$\text{net flow out of } i = \sum_{j=1}^{n} I_{ij} = 0.$$

The effective resistance of the circuit between the two probes is defined as

$$R_{\text{eff}} = (V_1 - V_n)/I$$

where I is the net amount of current flowing from 1 to n. If we choose our voltage-drop between the two probes so that the current from 1 to n to be 1, the effective resistance of the network will be given by $R_{\text{eff}} = V_1 - V_n$. Incorporating these facts, and substituting for I_{ij} in the current-conservation equations, leads to the following equation:

$$\sum_{j=1}^{n}(V_i - V_j)/R_{ij} = \begin{cases} 1 & \text{if } i = 1, \\ -1 & \text{if } i = n, \\ 0 & \text{otherwise.} \end{cases}$$

This can be written as a single matrix equation. Define the $n \times n$ matrix C by

$$c_{ij} = -R_{ij}^{-1} \quad (i \neq j), \qquad \text{and} \qquad c_{ii} = \sum_{j \neq i} R_{ij}^{-1}.$$

Thus the sum of the entries in any row or column of C is zero (use $R_{ij} = R_{ji}$). Our circuit equations can then be written as

$$Cv = q,$$

where the components of vector v are V_j, and the components of the vector q are $1, 0, 0, \ldots, 0, -1$. Note that the quantities R_{ij}^{-1} have physical significance; they are the *conductances* along the various wires. If i and j are not connected by a wire, you can say that the conductance R_{ij}^{-1} is zero (or that the resistance R_{ij} is "infinite").

We are interested in computing $R_{\text{eff}} = V_1 - V_n$. Note that if we add all n equations, we get the triviality $0 = 0$. This means that the last equation supplies no extra information; it is the negative of the sum of the other equations. Hence we can disregard the last row of C. Actually, we can make things even simpler. If we set $V_n = 0$ (i.e. assuming the potential at node n is zero), then we can forget about the last column of C as well. (The last column is irrelevant if V_n is zero, because then it will not contribute to q.)

Let C' denote what we get from C by removing its last row and column, and v' and q' the vectors v and q without their last components. Then $C'v' = q'$ or

$$v' = C'^{-1} q'.$$

We want to know the first entry of v'. We use a famous formula called Cramer's Rule. It says that the kth component of v' can be written as the ratio of two determinants: the numerator is the determinant of C' with its kth column replaced by q'; the denominator is the determinant of C' itself.

Thus

$$R_{\text{eff}} = \det(C'') \,/\, \det(C'),$$

where C'' is obtained from C' by replacing its first column by q'.

For example, consider the circuit shown in Figure 2, where all resistors have unit resistance. Then we obtain

Figure 2: A small circuit

Figure 3: A graph and one of its spanning trees

$$C = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}, \quad C' = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}, \quad C'' = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 3 & -1 \\ 0 & -1 & 3 \end{pmatrix}.$$

Hence $R_{\mathrm{eff}} = V_1 = \det(C'') \,/\, \det(C') = 8/8 = 1$.

By replacing the other columns of C' by the vector q' we determine $V_2 = V_3 = 1/2$. This gives us a check on our answer. For Ohm's Law then implies $I_{12} = I_{13} = I_{24} = I_{34} = 1/2$ and $I_{23} = 0$. This satisfies Kirkhoff's law at nodes 2 and 3, and has 1 ampere flowing out of node 1 and 1 ampere flowing into node 4.

Note that if we cross out the kth row and column of C, for *any* k between 1 and 4, we get a matrix with determinant 8. This may seem like just a numerical coincidence, but we will see in the next section that there is a strong reason for this to be true; namely, it is a consequence of the Matrix Tree Theorem.

2.2 Trees and the Matrix-Tree Theorem

Given n nodes, or vertices as we usually call them, a graph is a set of arcs (or edges), each arc being an (unordered) pair of vertices. Two vertices v and w in a graph G are *adjacent* if there is an edge between them. Two vertices v and w are connected by a path in G when there are arcs $(v, a), (a, b), \ldots, (c, d), (d, w)$ in G. A *spanning tree* is a graph T having $n - 1$ arcs so that there is a path from any one vertex to any other in T. A path in which the endpoints v and w coincide (and in which no other vertices are repeated) is called a cycle. It can be shown that a spanning tree has no cycles. See Figure 3.

Figure 4: Squeezing nodes a and b

If we take a graph G and squeeze two of its nodes a and b together, we get a new graph G_{ab}. (See Figure 4.)

Theorem 1 (Matrix-Tree Theorem) *The determinant of C' is given by*

$$S = \sum_T \prod_{(i,j)\in T} R_{ij}^{-1},$$

where the sum is over all spanning trees T in the original network.

We defer the proof to discuss consequences and applications.

The reader should first verify that the theorem is indeed true for the graph shown in Figure 2.

Next, note that there is nothing special about the node we happened to label 1; thus, if instead of eliminating the 1st row and column of C we eliminate the kth, the determinant of the sub-matrix will still be S. We use this fact to show that the determinant of C'' is given by the same formula, with the network $\bar{G} = G_{1n}$ playing the role of G. For, if we squeeze nodes 1 and n together (and call the resulting node node 1 of $\bar{G}$), the entries $\bar{c}_{ij}$ of the associated matrix $\bar{C}$ with $2 \le i, j \le n-1$ are equal to the corresponding entries c_{ij} of C''. If we throw out the first row and column of $\bar{C}$ we obtain a matrix $\bar{C}'$ whose determinant (by the above theorem) equals

$$\bar{S} = \sum_T \prod_{(i,j)\in T} R_{ij}^{-1},$$

where T ranges over all spanning trees of $\bar{G}$. But $\det(\bar{C}') = \det(C'')$, since C'' is of the form

$$\left(\begin{array}{c|c} 1 & * \cdots * \\ \hline 0 & \\ \vdots & \bar{C}' \\ 0 & \end{array}\right).$$

Hence $\det(C'') = \bar{S}$, as claimed.

Now, if the arc $(1,n)$ is in the original network G, then every spanning tree of $\bar{G}$ yields a spanning tree of G (by adding $(1,n)$), and conversely, every spanning tree T of G that contains the arc $(1,n)$ yields a spanning tree of $\bar{G}$. Thus

$$\bar{S} = R_{1n} \sum_{T \ni (1,n)} \prod_{(i,j) \in T} R_{ij}^{-1},$$

where T ranges over all spanning trees of G that contain the arc $(1,n)$. (Note that the R_{1n} cancels an unwanted factor of R_{1n}^{-1} that occurs in the product.) Thus the effective resistance of the network is

$$\frac{\det(C'')}{\det(C)} = \frac{\bar{S}}{S} = R_{1n} \frac{\sum_{T \ni (1,n)} \prod_{(i,j) \in T} R_{ij}^{-1}}{\sum_T \prod_{(i,j) \in T} R_{ij}^{-1}}.$$

That is, R is equal to R_{1n} times the proportion of the sum in Theorem 1 coming from trees containing the arc $(1,n)$. For example, you should check that in the example shown in Figure 2, the effective resistance between vertices 1 and 2 is $5/8$.

Corollary 1 *Assume unit resistances and an arc between the terminals 1 and n. Then the effective resistance R is given by the proportion of spanning trees of G containing $(1,n)$.*

One can often use the above statements to compute the resistance of circuits between pairs of points. This is easiest when there is some symmetry. For example, if each arc lies in the same number of trees, and the non-infinite R_{ij}'s are all equal, then the contribution from trees containing $(1,n)$ is the same as the contribution coming from trees containing any other arc, and must therefore be $n-1$ (the total number of vertices) divided by the total number of arcs.

For instance, consider the complete graph on n vertices (that is, a graph on n vertices with an edge joining every pair of distinct points); think of the edges as representing resistors, each having resistance 1. Each tree has $n-1$ arcs, or a proportion $2/n$ of the arcs, so each arc must occur in a proportion $2/n$ of the trees. Hence the total resistance between two vertices is $2/n$. For a graph with n vertices in one part and m in another and all mn arcs between the two parts (a "complete bipartite" graph), again with unit resistances, we have effective resistance $(n+m-1)/nm$, by the same reasoning: each tree contains this proportion of the arcs, so that each arc must occur in this proportion of trees.

Note that in general, one can always think of a resistive circuit as being represented by a graph, with labels on the edges that indicate the resistances of the associated resistors. In fact, one can use a complete graph, if one is careful to assign infinite resistance to all of the edges that don't correspond to resistors in the circuit.

For the infinite rectangular grid of unit resistors we get total resistance of 1/2 between adjacent nodes. A rigorous proof of this assertion lies beyond the scope of this course, but here is a heuristic argument. Let N denote the number of nodes in an infinite square grid (never mind that N is infinite!). There are $2N$ arcs altogether (a rightward and an upward arc from each node), each like every other, and a spanning tree has $N-1$ arcs. So by symmetry each arc lies in a proportion of $(N-1)/2N$ of the spanning trees, implying that the effective resistance between adjacent nodes of the network is $(N-1)/2N = 1/2$.

2.3 Proof of the Matrix-Tree Theorem.

We introduce new variables (or indeterminates, if you prefer) $x_1, x_2, \ldots, x_n$. We form the matrix $C'(x)$ by replacing R_{ij}^{-1} by $x_j R_{ij}^{-1}$ wherever the former expression occurs in C'. Explicitly this means that x_j appears as a factor in all off-diagonal elements in the jth column, and as a factor in a term in the ith diagonal element of $C(x)$ for all i such that nodes i and j are adjacent in the network. (The "x" in the notation is shorthand for "$x_1, x_2, ..., x_n$".)

Among trees, we introduce our variables as follows: For each tree T and each arc (i,j) in T, we multiply its contribution to the sum S by a factor of x_j whenever j is closer to n (the "root") than i is in the tree T. (Our insistence on discriminating between i and j based on closeness to n is just a device for making sure we count each edge of the tree exactly once, rather than twice.) This yields a polynomial we shall call $S(x)$. We will prove below the polynomial identity identity

$$\det(C'(x)) = S(x),$$

asserting the equality of two polynomials in the variables $x_1, ..., x_n$. By setting all $x_i = 1$, we can prove the desired equation $\det C' = S$ as a special case.

Before we try to prove $\det(C'(x)) = S(x)$ in the general case, let us look at the case $n = 3$. That is, we have a graph G on three nodes 1, 2 and 3 with resistance $R_{ij} = R_{ji}$ between nodes i and j (for all $i \neq j$). On the one hand we have

$$C(x) = \begin{pmatrix} x_2 R_{12}^{-1} + x_3 R_{13}^{-1} & -x_2 R_{12}^{-1} & -x_3 R_{13}^{-1} \\ -x_1 R_{12}^{-1} & x_1 R_{12}^{-1} + x_3 R_{23}^{-1} & -x_3 R_{23}^{-1} \\ -x_1 R_{13}^{-1} & -x_2 R_{23}^{-1} & x_1 R_{13}^{-1} + x_2 R_{23}^{-1} \end{pmatrix},$$

so that

$$\begin{aligned} \det(C'(x)) &= \begin{vmatrix} x_2 R_{12}^{-1} + x_3 R_{13}^{-1} & -x_2 R_{12}^{-1} \\ -x_1 R_{12}^{-1} & x_1 R_{12}^{-1} + x_3 R_{23}^{-1} \end{vmatrix} \\ &= x_1 x_3 R_{12}^{-1} R_{13}^{-1} + x_2 x_3 R_{12}^{-1} R_{23}^{-1} + x_3^2 R_{13}^{-1} R_{23}^{-1}. \end{aligned}$$

Figure 5: A graph and all of its spanning trees

On the other hand, G has three spanning trees, which are shown in Figure 5 with each arc oriented towards the node that is closer to the root node 3. The three trees respectively contribute $x_1 x_3 R_{12}^{-1} R_{13}^{-1}$, $x_2 x_3 R_{12}^{-1} R_{23}^{-1}$, and $x_3^2 R_{13}^{-1} R_{23}^{-1}$, whose sum is the determinant of $C'(x)$.

The way one proves a polynomial identity is by verifying that the coefficients of all monomials on one side of the identity are equal to what they are on the other. Both sides of this identity are polynomials of degree $n-1$ in the n variables. Thus, every monomial that appears has at least one variable that doesn't appear in it. We shall show that the coefficients of all monomials that have no x_k factor are the same for the tree sum $S(x)$ and for the determinant $\det(C'(x))$.

Every monomial has x_n in it: this is true for $S(x)$ since every tree has some arc which includes vertex n and thus gives a factor x_n; it is also true for $\det(C'(x))$ since the determinant vanishes if x_n is zero, all row sums then being zero.

So fix $k < n$ and consider setting $x_k = 0$. The terms in the determinant that survive are those without variable x_k. All off-diagonal terms in the kth column of C' are killed with $x_k = 0$, so the determinant of C' becomes c_{kk} times the determinant obtained with the kth row and column removed and x_k set to 0. (Recall that $c_{kk} = \sum_j R_{kj}^{-1} x_j$.)

The trees that contribute when x_k is set to 0 are those for which the kth node is not closer to the nth than any adjacent vertex: these are precisely the trees for which the kth node is a *leaf*. But the trees for which the kth node is a leaf will still be trees if the kth node is ignored; the contribution from these is therefore the same as the contribution we would get if there were no kth node, multiplied by a factor which measures the effect of reconnecting the kth node as a leaf to the rest of the tree.

Connecting the kth node as a leaf has the effect of increasing the degree of the node j it connects to by 1, which multiplies its contribution to our sum by $R_{kj}^{-1} x_j$. The different trees obtained by connecting the kth node as a leaf to each of the other nodes therefore produce an additional factor of $\sum_j R_{kj}^{-1} x_j$ that multiplies the contributions from the tree sums present without the kth vertex. Therefore the tree sum with $x_k = 0$ is what it would be without any kth vertex at all, multiplied by $\sum_j R_{kj}^{-1} x_j$.

The correctness of the terms with $x_k = 0$ now follows by induction. (The base case for the induction is a triviality that you should check for yourself.) We assume, for induction, that the sum of the terms in the determinant would equal the tree sum if there were no kth vertex. We have just shown that the effect of having a kth vertex when $x_k = 0$, both for tree sums and determinant, is to multiply what one had without that vertex (which must be identical by our induction hypothesis) by the same factor of $\sum R_{kj}^{-1} x_j$. But then all monomials without x_k in them have the same coefficients on both sides of the identity, for any k other than n; hence all coefficients agree, which proves the theorem.

Notice what we achieved here by introducing the variables x_j. At first glance they seem to complicate things. However we were able to see what happens when one of them is set equal to zero. Furthermore, they allow us to break the sums and determinant up into parts which don't vanish when one variable is set equal to zero. Without them we would have had to treat all the terms at once. It is much easier to prove the result one monomial at a time (or to prove it for all monomials lacking a specific variable at one time, as we have done above), than to try to prove the whole thing at once. □

Exercises.

1. Assume unit resistances. Find the effective resistance between adjacent vertices in the regular cube, regular icosahedron and in the regular dodecahedron. Do the same for the infinite hexagonal and triangular grids.

2. Let G be the 4-node electrical network shown in Figure 2 of the text. Assume all resistors have resistance 1 ohm. For *every* pair of nodes in the network, use the Matrix-Tree Theorem or its corollary to find the effective resistance between them.

3. **(a)** Assume unit resistances between *every* pair of nodes. Show that the determinant of $C'(x)$ becomes $x_n(x_1 + x_2 + \ldots + x_n)^{n-2}$. (Hint: In proving this you may use the same argument used here for proof of the matrix-tree theorem: namely, you may use induction to verify that for all k the coefficients in which x_k does not occur (which are precisely those that survive when $x_k = 0$), are correct, and then "notice" that this assertion proves the claim.)

(b) From this, deduce a formula for the total number of spanning trees on the complete graph on n nodes.

4. Consider the two circuits shown below:

Resistances are as labeled; e.g., $R_{ux} = a$. Use the matrix-tree theorem to show that the effective resistance between u' and w' is equal to the effective resistance between u and w, provided that we set $a' = bc/(a+b+c)$, $b' = ac/(a+b+c)$, and $c' = ab/(a+b+c)$. (Note that by symmetry, the same choice of a', b', c' will also make $R_{\text{eff}}(u', w') = R_{\text{eff}}(u, w)$ and $R_{\text{eff}}(v', w') = R_{\text{eff}}(v, w)$.) This fact is called the *triangle-star relation*, and it plays an important role in certain aspects of modern theoretical physics.