An Introduction to Combinatorics and Graph Theory

David Guichard

This copy of the text was compiled from source at 11:36 on 3/4/2023.

We will be glad to receive corrections and suggestions for improvement at guichard@whitman.edu.

Contents

3

4

5

6

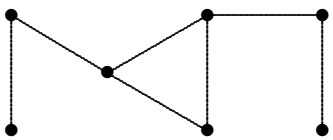
A

1

Fundamentals

Combinatorics is often described briefly as being about counting, and indeed counting is a large part of combinatorics. As the name suggests, however, it is broader than this: it is about combining things. Questions that arise include counting problems: "How many ways can these elements be combined?" But there are other questions, such as whether a certain combination is possible, or what combination is the "best" in some sense. We will see all of these, though counting plays a particularly large role.

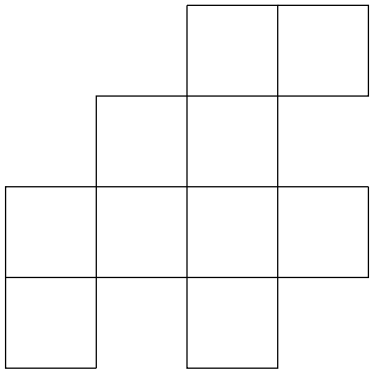
Graph theory is concerned with various types of networks, or really models of networks called graphs. These are not the graphs of analytic geometry, but what are often described as "points connected by lines", for example:



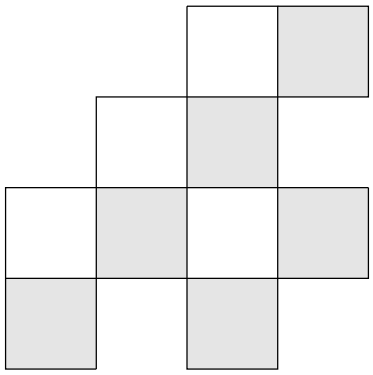
The preferred terminology is **vertex** for a point and **edge** for a line. The lines need not be straight lines, and in fact the actual definition of a graph is not a geometric definition. The figure above is simply a visualization of a graph; the graph is a more abstract object, consisting of seven vertices, which we might name $\{v_1, \ldots, v_7\}$, and the collection of pairs of vertices that are connected; for a suitable assignment of names v_i to the points in the diagram, the edges could be represented as $\{v_1, v_2\}$,$\{v_2, v_3\}$,$\{v_3, v_4\}$,$\{v_3, v_5\}$,$\{v_4, v_5\}$, $\{v_5, v_6\}$,$\{v_6, v_7\}$.

1.1 Examples

Suppose we have a chess board, and a collection of tiles, like dominoes, each of which is the size of two squares on the chess board. Can the chess board be covered by the dominoes? First we need to be clear on the rules: the board is covered if the dominoes are laid down so that each covers exactly two squares of the board; no dominoes overlap; and every square is covered. The answer is easy: simply by laying out 32 dominoes in rows, the board can be covered. To make the problem more interesting, we allow the board to be rectangular of any size, and we allow some squares to be removed from the board. What can be say about whether the remaining board can be covered? This is such a board, for example:

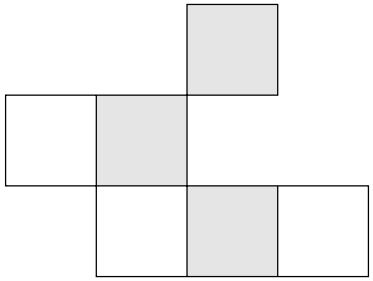


What can we say? Here is an easy observation: each domino must cover two squares, so the total number of squares must be even; the board above has an even number of squares. Is that enough? It is not too hard to convince yourself that this board cannot be covered; is there some general principle at work? Suppose we redraw the board to emphasize that it really is part of a chess board:

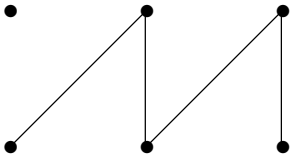


Aha! Every tile must cover one white and one gray square, but there are four of the former and six of the latter, so it is impossible. Now do we have the whole picture? No;

for example:

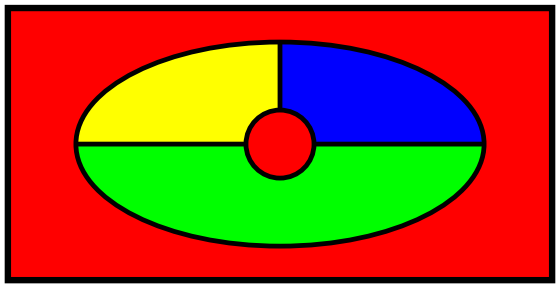


The gray square at the upper right clearly cannot be covered. Unfortunately it is not easy to state a condition that fully characterizes the boards that can be covered; we will see this problem again. Let us note, however, that this problem can also be represented as a graph problem. We introduce a vertex corresponding to each square, and connect two vertices by an edge if their associated squares can be covered by a single domino; here is the previous board:



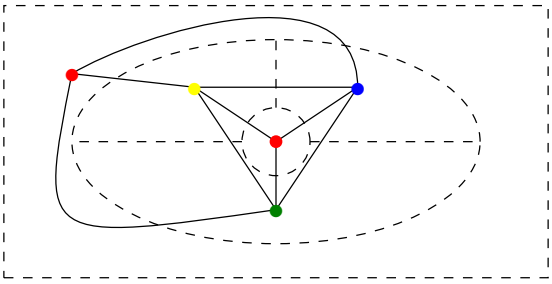
Here the top row of vertices represents the gray squares, the bottom row the white squares. A domino now corresponds to an edge; a covering by dominoes corresponds to a collection of edges that share no endpoints and that are **incident** with (that is, touch) all six vertices. Since no edge is incident with the top left vertex, there is no cover.

Perhaps the most famous problem in graph theory concerns map coloring: Given a map of some countries, how many colors are required to color the map so that countries sharing a border get different colors? It was long conjectured that any map could be colored with four colors, and this was finally proved in 1976. Here is an example of a small map, colored with four colors:

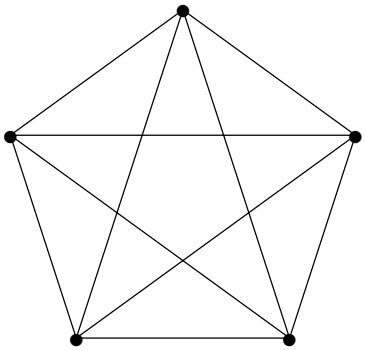


Typically this problem is turned into a graph theory problem. Suppose we add to each country a capital, and connect capitals across common boundaries. Coloring the capitals so

that no two connected capitals share a color is clearly the same problem. For the previous map:



Any graph produced in this way will have an important property: it can be drawn so that no edges cross each other; this is a **planar** graph. Non-planar graphs can require more than four colors, for example this graph:



This is called the **complete graph** on five vertices, denoted K_5; in a complete graph, each vertex is connected to each of the others. Here only the "fat" dots represent vertices; intersections of edges at other points are not vertices. A few minutes spent trying should convince you that this graph cannot be drawn so that its edges don't cross, though the number of edge crossings can be reduced.

Exercises 1.1.

1. Explain why an $m \times n$ board can be covered if either m or n is even. Explain why it cannot be covered if both m and n are odd.
2. Suppose two diagonally opposite corners of an ordinary 8×8 board are removed. Can the resulting board be covered?
3. Suppose that m and n are both odd. On an $m \times n$ board, colored as usual, all four corners will be the same color, say white. Suppose one white square is removed from any location on the board. Show that the resulting board can be covered.
4. Suppose that one corner of an 8×8 board is removed. Can the remainder be covered by 1×3 tiles? Show a tiling or prove that it cannot be done.

5. Suppose the square in row 3, column 3 of an 8×8 board is removed. Can the remainder be covered by 1×3 tiles? Show a tiling or prove that it cannot be done.

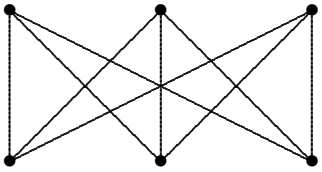
6. Remove two diagonally opposite corners of an $m \times n$ board, where m is odd and n is even. Show that the remainder can be covered with dominoes.

7. Suppose one white and one black square are removed from an $n \times n$ board, n even. Show that the remainder can be covered by dominoes.

8. Suppose an $n \times n$ board, n even, is covered with dominoes. Show that the number of horizontal dominoes with a white square under the left end is equal to the number of horizontal dominoes with a black square under the left end.

9. In the complete graph on five vertices shown above, there are five pairs of edges that cross. Draw this graph so that only one pair of edges cross. Remember that "edges" do not have to be straight lines.

10. The **complete bipartite graph** $K_{3,3}$ consists of two groups of three vertices each, with all possible edges between the groups and no other edges:



Draw this graph with only one crossing.

1.2 Combinations and permutations

We turn first to *counting*. While this sounds simple, perhaps too simple to study, it is not. When we speak of counting, it is shorthand for determining the size of a set, or more often, the sizes of many sets, all with something in common, but different sizes depending on one or more parameters. For example: how many outcomes are possible when a die is rolled? Two dice? n dice? As stated, this is ambiguous: what do we mean by "outcome"? Suppose we roll two dice, say a red die and a green die. Is "red two, green three" a different outcome than "red three, green two"? If yes, we are counting the number of possible "physical" outcomes, namely 36. If no, there are 21. We might even be interested simply in the possible totals, in which case there are 11 outcomes.

Even the quite simple first interpretation relies on some degree of knowledge about counting; we first make two simple facts explicit. In terms of set sizes, suppose we know that set A has size m and set B has size n. What is the size of A and B together, that is, the size of $A \cup B$? If we know that A and B have no elements in common, then the size $A \cup B$ is $m + n$; if they do have elements in common, we need more information. A simple but typical problem of this type: if we roll two dice, how many ways are there to get either 7 or 11? Since there are 6 ways to get 7 and two ways to get 11, the answer is $6 + 2 = 8$. Though this principle is simple, it is easy to forget the requirement that the two sets be

disjoint, and hence to use it when the circumstances are otherwise. This principle is often called the **addition principle**.

This principle can be generalized: if sets A_1 through A_n are pairwise disjoint and have sizes $m_1, \ldots m_n$, then the size of $A_1 \cup \cdots \cup A_n = \sum_{i=1}^{n} m_i$. This can be proved by a simple induction argument.

Why do we know, without listing them all, that there are 36 outcomes when two dice are rolled? We can view the outcomes as two separate outcomes, that is, the outcome of rolling die number one and the outcome of rolling die number two. For each of 6 outcomes for the first die the second die may have any of 6 outcomes, so the total is $6+6+6+6+6+6 = 36$, or more compactly, $6 \cdot 6 = 36$. Note that we are really using the addition principle here: set A_1 is all pairs $(1, x)$, set A_2 is all pairs $(2, x)$, and so on. This is somewhat more subtle than is first apparent. In this simple example, the outcomes of die number two have nothing to do with the outcomes of die number one. Here's a slightly more complicated example: how many ways are there to roll two dice so that the two dice don't match? That is, we rule out 1-1, 2-2, and so on. Here for each possible value on die number one, there are five possible values for die number two, but they are a different five values for each value on die number one. Still, because all are the same, the result is $5+5+5+5+5+5 = 30$, or $6 \cdot 5 = 30$. In general, then, if there are m possibilities for one event, and n for a second event, the number of possible outcomes for both events together is $m \cdot n$. This is often called the **multiplication principle**.

In general, if n events have m_i possible outcomes, for $i = 1, \ldots, n$, where each m_i is unaffected by the outcomes of other events, then the number of possible outcomes overall is $\prod_{i=1}^{n} m_i$. This too can be proved by induction.

EXAMPLE 1.2.1 How many outcomes are possible when three dice are rolled, if no two of them may be the same? The first two dice together have $6 \cdot 5 = 30$ possible outcomes, from above. For each of these 30 outcomes, there are four possible outcomes for the third die, so the total number of outcomes is $30 \cdot 4 = 6 \cdot 5 \cdot 4 = 120$. (Note that we consider the dice to be distinguishable, that is, a roll of 6, 4, 1 is different than 4, 6, 1, because the first and second dice are different in the two rolls, even though the numbers as a set are the same.) □

EXAMPLE 1.2.2 Suppose blocks numbered 1 through n are in a barrel; we pull out k of them, placing them in a line as we do. How many outcomes are possible? That is, how many different arrangements of k blocks might we see?

This is essentially the same as the previous example: there are k "spots" to be filled by blocks. Any of the n blocks might appear first in the line; then any of the remaining $n-1$ might appear next, and so on. The number of outcomes is thus $n(n-1)(n-2)\cdots(n-k+1)$, by the multiplication principle. In the previous example, the first "spot" was die number

one, the second spot was die number two, the third spot die number three, and $6 \cdot 5 \cdot 4 = 6(6-1)(6-2)$; notice that $6 - 2 = 6 - 3 + 1$. □

This is quite a general sort of problem:

DEFINITION 1.2.3 The number of permutations of n things taken k at a time is

$$P(n,k) = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

□

A permutation of some objects is a particular linear ordering of the objects; $P(n,k)$ in effect counts two things simultaneously: the number of ways to choose and order k out of n objects. A useful special case is $k = n$, in which we are simply counting the number of ways to order all n objects. This is $n(n-1)\cdots(n-n+1) = n!$. Note that the second form of $P(n,k)$ from the definition gives

$$\frac{n!}{(n-n)!} = \frac{n!}{0!}.$$

This is correct only if $0! = 1$, so we adopt the standard convention that this is true, that is, we *define* 0! to be 1.

Suppose we want to count only the number of ways to choose k items out of n, that is, we don't care about order. In example 1.2.1, we counted the number of rolls of three dice with different numbers showing. The dice were distinguishable, or in a particular order: a first die, a second, and a third. Now we want to count simply how many combinations of numbers there are, with 6, 4, 1 now counting as the same combination as 4, 6, 1.

EXAMPLE 1.2.4 Suppose we were to list all 120 possibilities in example 1.2.1. The list would contain many outcomes that we now wish to count as a single outcome; 6, 4, 1 and 4, 6, 1 would be on the list, but should not be counted separately. How many times will a single outcome appear on the list? This is a permutation problem: there are 3! orders in which 1, 4, 6 can appear, and all 6 of these will be on the list. In fact every outcome will appear on the list 6 times, since every outcome can appear in 3! orders. Hence, the list is too big by a factor of 6; the correct count for the new problem is $120/6 = 20$. □

Following the same reasoning in general, if we have n objects, the number of ways to choose k of them is $P(n,k)/k!$, as each collection of k objects will be counted $k!$ times by $P(n,k)$.

DEFINITION 1.2.5 The number of subsets of size k of a set of size n (also called an n-set) is

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

The notation $C(n,k)$ is rarely used; instead we use $\binom{n}{k}$, pronounced "n choose k". □

EXAMPLE 1.2.6 Consider $n = 0, 1, 2, 3$. It is easy to list the subsets of a small n-set; a typical n-set is $\{a_1, a_2, \ldots, a_n\}$. A 0-set, namely the empty set, has one subset, the empty set; a 1-set has two subsets, the empty set and $\{a_1\}$; a 2-subset has four subsets, $\emptyset$, $\{a_1\}$, $\{a_2\}$, $\{a_1, a_2\}$; and a 3-subset has eight: $\emptyset$, $\{a_1\}$, $\{a_2\}$, $\{a_3\}$, $\{a_1, a_2\}$, $\{a_1, a_3\}$, $\{a_2, a_3\}$, $\{a_1, a_2, a_3\}$. From these lists it is then easy to compute $\binom{n}{k}$:

		k			
		0	1	2	3
	0	1			
n	1	1	1		
	2	1	2	1	
	3	1	3	3	1

□

You probably recognize these numbers: this is the beginning of **Pascal's Triangle**. Each entry in Pascal's triangle is generated by adding two entries from the previous row: the one directly above, and the one above and to the left. This suggests that $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, and indeed this is true. To make this work out neatly, we adopt the convention that $\binom{n}{k} = 0$ when $k < 0$ or $k > n$.

THEOREM 1.2.7 $\displaystyle\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$

Proof. A typical n-set is $A = \{a_1, \ldots, a_n\}$. We consider two types of subsets: those that contain a_n and those that do not. If a k-subset of A does not contain a_n, then it is a k-subset of $\{a_1, \ldots, a_{n-1}\}$, and there are $\binom{n-1}{k}$ of these. If it does contain a_n, then it consists of a_n and $k-1$ elements of $\{a_1, \ldots, a_{n-1}\}$; since there are $\binom{n-1}{k-1}$ of these, there are $\binom{n-1}{k-1}$ subsets of this type. Thus the total number of k-subsets of A is $\binom{n-1}{k-1} + \binom{n-1}{k}$.

Note that when $k = 0$, $\binom{n-1}{k-1} = \binom{n-1}{-1} = 0$, and when $k = n$, $\binom{n-1}{k} = \binom{n-1}{n} = 0$, so that $\binom{n}{0} = \binom{n-1}{0}$ and $\binom{n}{n} = \binom{n-1}{n-1}$. These values are the boundary ones in Pascal's Triangle. ■

Many counting problems rely on the sort of reasoning we have seen. Here are a few variations on the theme.

EXAMPLE 1.2.8 Six people are to sit at a round table; how many seating arrangements are there?

It is not clear exactly what we mean to count here. If there is a "special seat", for example, it may matter who ends up in that seat. If this doesn't matter, we only care about the relative position of each person. Then it may or may not matter whether a certain person is on the left or right of another. So this question can be interpreted in (at least) three ways. Let's answer them all.

First, if the actual chairs occupied by people matter, then this is exactly the same as lining six people up in a row: 6 choices for seat number one, 5 for seat two, and so on, for a total of 6!. If the chairs don't matter, then 6! counts the same arrangement too many times, once for each person who might be in seat one. So the total in this case is $6!/6 = 5!$. Another approach to this: since the actual seats don't matter, just put one of the six people in a chair. Then we need to arrange the remaining 5 people in a row, which can be done in 5! ways. Finally, suppose all we care about is who is next to whom, ignoring right and left. Then the previous answer counts each arrangement twice, once for the counterclockwise order and once for clockwise. So the total is $5!/2 = P(5,3)$. □

We have twice seen a general principle at work: if we can overcount the desired set in such a way that every item gets counted the same number of times, we can get the desired count just by dividing by the common overcount factor. This will continue to be a useful idea. A variation on this theme is to overcount and then *subtract* the amount of overcount.

EXAMPLE 1.2.9 How many ways are there to line up six people so that a particular pair of people are not adjacent?

Denote the people A and B. The total number of orders is 6!, but this counts those orders with A and B next to each other. How many of these are there? Think of these two people as a unit; how many ways are there to line up the AB unit with the other 4 people? We have 5 items, so the answer is 5!. Each of these orders corresponds to two different orders in which A and B are adjacent, depending on whether A or B is first. So the 6! count is too high by $2 \cdot 5!$ and the count we seek is $6! - 2 \cdot 5! = 4 \cdot 5!$. □

Exercises 1.2.

1. How many positive factors does $2 \cdot 3^4 \cdot 7^3 \cdot 11^2 \cdot 47^5$ have? How many does $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ have, where the p_i are distinct primes?

2. A poker hand consists of five cards from a standard 52 card deck with four suits and thirteen values in each suit; the order of the cards in a hand is irrelevant. How many hands consist of 2 cards with one value and 3 cards of another value (a full house)? How many consist of 5 cards from the same suit (a flush)?

3. Six men and six women are to be seated around a table, with men and women alternating. The chairs don't matter, only who is next to whom, but right and left are different. How many seating arrangements are possible?
4. Eight people are to be seated around a table; the chairs don't matter, only who is next to whom, but right and left are different. Two people, X and Y, cannot be seated next to each other. How many seating arrangements are possible?
5. In chess, a rook attacks any piece in the same row or column as the rook, provided no other piece is between them. In how many ways can eight indistinguishable rooks be placed on a chess board so that no two attack each other? What about eight indistinguishable rooks on a 10×10 board?
6. Suppose that we want to place 8 non-attacking rooks on a chessboard. In how many ways can we do this if the 16 most 'northwest' squares must be empty? How about if only the 4 most 'northwest' squares must be empty?
7. A "legal" sequence of parentheses is one in which the parentheses can be properly matched, like ()(()). It's not hard to see that this is possible precisely when the number of left and right parentheses is the same, and every initial segment of the sequence has at least as many left parentheses as right. For example, ()) . . . cannot possibly be extended to a legal sequence. Show that the number of legal sequences of length $2n$ is $C_n = \binom{2n}{n} - \binom{2n}{n+1}$. The numbers C_n are called the **Catalan numbers**.

1.3 Binomial coefficients

Recall the appearance of Pascal's Triangle in example 1.2.6. If you have encountered the triangle before, you may know it has many interesting properties. We will explore some of these here.

You may know, for example, that the entries in Pascal's Triangle are the coefficients of the polynomial produced by raising a binomial to an integer power. For example, $(x+y)^3 = 1 \cdot x^3 + 3 \cdot x^2 y + 3 \cdot xy^2 + 1 \cdot y^3$, and the coefficients 1, 3, 3, 1 form row three of Pascal's Triangle. For this reason the numbers $\binom{n}{k}$ are usually referred to as the **binomial coefficients**.

THEOREM 1.3.1 Binomial Theorem

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n = \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i$$

Proof. We prove this by induction on n. It is easy to check the first few, say for $n = 0, 1, 2$, which form the base case. Now suppose the theorem is true for $n-1$, that is,

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

Then

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

Using the distributive property, this becomes

$$x\sum_{i=0}^{n-1}\binom{n-1}{i}x^{n-1-i}y^i + y\sum_{i=0}^{n-1}\binom{n-1}{i}x^{n-1-i}y^i$$
$$= \sum_{i=0}^{n-1}\binom{n-1}{i}x^{n-i}y^i + \sum_{i=0}^{n-1}\binom{n-1}{i}x^{n-1-i}y^{i+1}.$$

These two sums have much in common, but it is slightly disguised by an "offset": the first sum starts with an $x^n y^0$ term and ends with an $x^1 y^{n-1}$ term, while the corresponding terms in the second sum are $x^{n-1}y^1$ and $x^0 y^n$. Let's rewrite the second sum so that they match:

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

Now we can use theorem 1.2.7 to get:

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

At the next to last step we used the facts that $\binom{n-1}{0} = \binom{n}{0}$ and $\binom{n-1}{n-1} = \binom{n}{n}$. ∎

Here is an interesting consequence of this theorem: Consider

$$(x+y)^n = (x+y)(x+y)\cdots(x+y).$$

One way we might think of attempting to multiply this out is this: Go through the n factors $(x+y)$ and in each factor choose either the x or the y; at the end, multiply your

choices together, getting some term like $xxyxyy\cdots yx = x^i y^j$, where of course $i+j=n$. If we do this in all possible ways and then collect like terms, we will clearly get

$$\sum_{i=0}^{n} a_i x^{n-i} y^i.$$

We know that the correct expansion has $\binom{n}{i} = a_i$; is that in fact what we will get by this method? Yes: consider $x^{n-i}y^i$. How many times will we get this term using the given method? It will be the number of times we end up with i y-factors. Since there are n factors $(x+y)$, the number of times we get i y-factors must be the number of ways to pick i of the $(x+y)$ factors to contribute a y, namely $\binom{n}{i}$. This is probably not a useful method in practice, but it is interesting and occasionally useful.

EXAMPLE 1.3.2 Using this method we might get

$$(x+y)^3 = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$

which indeed becomes $x^3 + 3x^2y + 3xy^2 + y^3$ upon collecting like terms. □

The Binomial Theorem, 1.3.1, can be used to derive many interesting identities. A common way to rewrite it is to substitute $y = 1$ to get

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

If we then substitute $x = 1$ we get

$$2^n = \sum_{i=0}^{n} \binom{n}{i},$$

that is, row n of Pascal's Triangle sums to 2^n. This is also easy to understand combinatorially: the sum represents the total number of subsets of an n-set, since it adds together the numbers of subsets of every possible size. It is easy to see directly that the number of subsets of an n-set is 2^n: for each element of the set we make a choice, to include or to exclude the element. The total number of ways to make these choices is $2\cdot 2\cdots 2 = 2^n$, by the multiplication principle.

Suppose now that $n \geq 1$ and we substitute -1 for x; we get

$$(-1+1)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i}. \tag{1.3.1}$$

The sum is now an alternating sum: every other term is multiplied by -1. Since the left hand side is 0, we can rewrite this to get

$$\binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots. \tag{1.3.2}$$

So each of these sums is 2^{n-1}.

Another obvious feature of Pascal's Triangle is symmetry: each row reads the same forwards and backwards. That is, we have:

THEOREM 1.3.3 $\binom{n}{i} = \binom{n}{n-i}$.

Proof. This is quite easy to see combinatorially: every i-subset of an n-set is associated with an $(n-i)$-subset. That is, if the n-set is A, and if $B \subseteq A$ has size i, then the complement of B has size $n-i$. This establishes a 1–1 correspondence between sets of size i and sets of size $n-i$, so the numbers of each are the same. (Of course, if $i = n-i$, no proof is required.) ■

Note that this means that the Binomial Theorem, 1.3.1, can also be written as

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

or

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

Another striking feature of Pascal's Triangle is that the entries across a row are strictly increasing to the middle of the row, and then strictly decreasing. Since we already know that the rows are symmetric, the first part of this implies the second.

THEOREM 1.3.4 For $1 \le i \le \lfloor \frac{n}{2} \rfloor$, $\binom{n}{i} > \binom{n}{i-1}$.

Proof. This is by induction; the base case is apparent from the first few rows. Write

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$$
$$\binom{n}{i-1} = \binom{n-1}{i-2} + \binom{n-1}{i-1}$$

Provided that $1 \le i \le \lfloor \frac{n-1}{2} \rfloor$, we know by the induction hypothesis that

$$\binom{n-1}{i} > \binom{n-1}{i-1}.$$

Provided that $1 \le i-1 \le \lfloor \frac{n-1}{2} \rfloor$, or equivalently $2 \le i \le \lfloor \frac{n-1}{2} \rfloor + 1$, we know that

$$\binom{n-1}{i-1} > \binom{n-1}{i-2}.$$

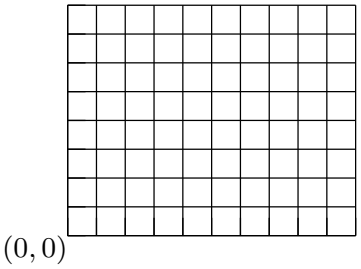
Hence if $2 \le i \le \lfloor \frac{n-1}{2} \rfloor$,

$$\binom{n}{i} > \binom{n}{i-1}.$$

This leaves two special cases to check: $i = 1$ and for n even, $i = \lfloor \frac{n-1}{2} \rfloor + 1 = \lfloor \frac{n}{2} \rfloor$. These are left as an exercise. ■

Exercises 1.3.

1. Suppose a street grid starts at position $(0,0)$ and extends up and to the right:



A shortest route along streets from $(0,0)$ to (i,j) is $i+j$ blocks long, going i blocks east and j blocks north. How many such routes are there? Suppose that the block between (k,l) and $(k+1,l)$ is closed, where $k<i$ and $l \le j$. How many shortest routes are there from $(0,0)$ to (i,j)?

2. Prove by induction that $\sum_{k=0}^{n} \binom{k}{i} = \binom{n+1}{i+1}$ for $n \ge 0$ and $i \ge 0$.

3. Use a combinatorial argument to prove that $\sum_{k=0}^{n} \binom{k}{i} = \binom{n+1}{i+1}$ for $n \ge 0$ and $i \ge 0$; that is, explain why the left-hand side counts the same thing as the right-hand side.

4. Use a combinatorial argument to prove that $\binom{k}{2} + \binom{n-k}{2} + k(n-k) = \binom{n}{2}$.

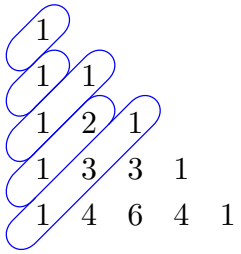
5. Use a combinatorial argument to prove that $\binom{2n}{n}$ is even.

6. Suppose that A is a non-empty finite set. Prove that A has as many even-sized subsets as it does odd-sized subsets.

7. Prove that $\sum_{k=0}^{n} \binom{k}{i} k = \binom{n+1}{i+1} n - \binom{n+1}{i+2}$ for $n \ge 0$ and $i \ge 0$.

8. Verify that $\binom{n+1}{2} + \binom{n}{2} = n^2$. Use exercise 2 to find a simple expression for $\sum_{i=1}^{n} i^2$.

9. Make a conjecture about the sums of the upward diagonals in Pascal's Triangle as indicated. Prove your conjecture is true.



10. Find the number of ways to write n as an ordered sum of ones and twos, $n \ge 0$. For example, when $n=4$, there are five ways: $1+1+1+1$, $2+1+1$, $1+2+1$, $1+1+2$, and $2+2$.

11. Use $(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ to find a simple expression for $\sum_{i=1}^{n} i\binom{n}{i} x^{i-1}$. Then find a simple expression for $\sum_{i=1}^{n} i\binom{n}{i}$.

12. Use $(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ to find a simple expression for $\sum_{i=0}^{n} \frac{1}{i+1}\binom{n}{i} x^{i+1}$. Then find a simple expression for $\sum_{i=0}^{n} \frac{1}{i+1}\binom{n}{i}$.

13. Use the previous exercise to find a simple expression for $\sum_{i=0}^{n} (-1)^i \frac{1}{i+1}\binom{n}{i}$.

14. Give a combinatorial proof of

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

Rewrite this identity in simpler form if $m = n$, and when $k = m = n$.

15. Finish the proof of theorem 1.3.4.

16. Give an alternate proof of theorm 1.3.4 by characterizing those i for which $\binom{n}{i}/\binom{n}{i-1} > 1$.

17. When is $\binom{n}{i}/\binom{n}{i-1}$ a maximum? When is $\binom{n}{i}/\binom{n}{i-1} = 2$?

18. When is $\binom{n}{i} - \binom{n}{i-1}$ a maximum?

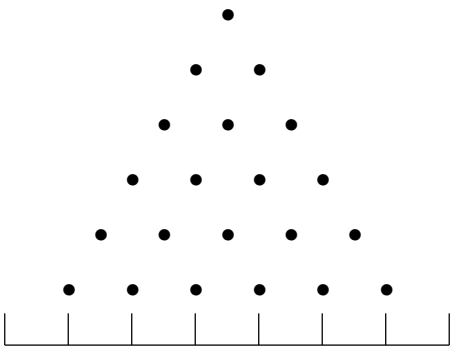
19. A **Galton board** is an upright flat surface with protruding horizontal pins arranged as shown below. At the bottom are a number of bins; if the number of rows is n, the number of bins is $n + 1$. A ball is dropped directly above the top pin, and at each pin bounces left or right with equal probability. We assume that the ball next hits the pin below and immediately left or right of the pin it has struck, and this continues down the board, until the ball falls into a bin at the bottom. If we number the bins from 0 to n, how many paths can a ball travel to end up in bin k?

This may be interpreted in terms of probability, which was the intent of Sir Francis Galton when he designed it. Each path is equally likely to be taken by a ball. If many balls are dropped, the number of balls in bin k corresponds to the probability of ending up in that bin. The more paths that end in a bin, the higher the probability. When a very large number of balls are dropped, the balls will form an approximation to the bell curve familiar from probability and statistics.

There is an animation of the process at

https://www.randomservices.org/random/apps/GaltonBoardExperiment.html.

There was once a very nice physical implementation at the Pacific Science Center in Seattle.



1.4 Bell numbers

We begin with a definition:

DEFINITION 1.4.1 A **partition** of a set S is a collection of non-empty subsets $A_i \subseteq S$, $1 \leq i \leq k$ (the **parts** of the partition), such that $\bigcup_{i=1}^{k} A_i = S$ and for every $i \neq j$, $A_i \cap A_j = \emptyset$. □

EXAMPLE 1.4.2 The partitions of the set $\{a, b, c\}$ are $\{\{a\}, \{b\}, \{c\}\}$, $\{\{a, b\}, \{c\}\}$, $\{\{a, c\}, \{b\}\}$, $\{\{b, c\}, \{a\}\}$, and $\{\{a, b, c\}\}$. □

Partitions arise in a number of areas of mathematics. For example, if $\equiv$ is an equivalence relation on a set S, the equivalence classes of $\equiv$ form a partition of S. Here we consider the number of partitions of a finite set S, which we might as well take to be $[n] = \{1, 2, 3, \ldots, n\}$, unless some other set is of interest. We denote the number of partitions of an n-element set by B_n; these are the **Bell** numbers. From the example above, we see that $B_3 = 5$. For convenience we let $B_0 = 1$. It is quite easy to see that $B_1 = 1$ and $B_2 = 2$.

There are no known simple formulas for B_n, so we content ourselves with a recurrence relation.

THEOREM 1.4.3 The Bell numbers satisfy

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

Proof. Consider a partition of $S = \{1, 2, \ldots, n+1\}$, $A_1, \ldots, A_m$. We may suppose that $n+1$ is in A_1, and that $|A_1| = k+1$, for some k, $0 \leq k \leq n$. Then $A_2, \ldots, A_m$ form a partition of the remaining $n-k$ elements of S, that is, of $S \backslash A_1$. There are B_{n-k} partitions of this set, so there are B_{n-k} partitions of S in which one part is the set A_1. There are $\binom{n}{k}$ sets of size $k+1$ containing $n+1$, so the total number of partitions of S in which $n+1$ is in a set of size $k+1$ is $\binom{n}{k} B_{n-k}$. Adding up over all possible values of k, this means

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}. \tag{1.4.1}$$

We may rewrite this, using theorem 1.3.3, as

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{n-k} B_{n-k},$$

and then notice that this is the same as the sum

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

written backwards. ■

EXAMPLE 1.4.4 We apply the recurrence to compute the first few Bell numbers:

$$B_1 = \sum_{k=0}^{0} \binom{0}{0} B_0 = 1 \cdot 1 = 1$$

$$B_2 = \sum_{k=0}^{1} \binom{1}{k} B_k = \binom{1}{0} B_0 + \binom{1}{1} B_1 = 1 \cdot 1 + 1 \cdot 1 = 1 + 1 = 2$$

$$B_3 = \sum_{k=0}^{2} \binom{2}{k} B_k = 1 \cdot 1 + 2 \cdot 1 + 1 \cdot 2 = 5$$

$$B_4 = \sum_{k=0}^{3} \binom{3}{k} B_k = 1 \cdot 1 + 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 5 = 15$$

□

The Bell numbers grow exponentially fast; the first few are 1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437.

The Bell numbers turn up in many other problems; here is an interesting example. A common need in some computer programs is to generate a random permutation of $1, 2, 3, \ldots, n$, which we may think of as a shuffle of the numbers, visualized as numbered cards in a deck. Here is an attractive method that is easy to program: Start with the numbers in order, then at each step, remove one number at random (this is easy in most programming languages) and put it at the front of the list of numbers. (Viewed as a shuffle of a deck of cards, this corresponds to removing a card and putting it on the top of the deck.) How many times should we do this? There is no magic number, but it certainly should not be small relative to the size of n. Let's choose n as the number of steps.

We can write such a shuffle as a list of n integers, $(m_1, m_2, \ldots, m_n)$. This indicates that at step i, the number m_i is moved to the front.

EXAMPLE 1.4.5 Let's follow the shuffle $(3, 2, 2, 4, 1)$:

$$\begin{aligned} (3): &\quad 31245 \\ (2): &\quad 23145 \\ (2): &\quad 23145 \\ (4): &\quad 42315 \\ (1): &\quad 14235 \end{aligned}$$

□

Note that we allow "do nothing" moves, removing the top card and then placing it on top. The number of possible shuffles is then easy to count: there are n choices for the card

to remove, and this is repeated n times, so the total number is n^n. (If we continue a shuffle for m steps, the number of shuffles is n^m.) Since there are only $n!$ different permutations of $1, 2, \ldots, n$, this means that many shuffles give the same final order.

Here's our question: how many shuffles result in the original order?

EXAMPLE 1.4.6 These shuffles return to the original order: $(1, 1, 1, 1, 1)$, $(5, 4, 3, 2, 1)$, $(4, 1, 3, 2, 1)$. □

THEOREM 1.4.7 The number of shuffles of $[n]$ that result in the original sorted order is B_n.

Proof. Since we know that B_n counts the number of partitions of $\{1, 2, 3, \ldots, n\}$, we can prove the theorem by establishing a 1–1 correspondence between the shuffles that leave the deck sorted and the partitions. Given a shuffle $(m_1, m_2, \ldots, m_n)$, we put into a single set all i such that m_i has a single value. For example, using the shuffle $(4, 1, 3, 2, 1)$, Since $m_2 = m_5$, one set is $\{2, 5\}$. All the other values are distinct, so the other sets in the partition are $\{1\}$, $\{3\}$, and $\{4\}$.

Note that every shuffle, no matter what the final order, produces a partition by this method. We are only interested in the shuffles that leave the deck sorted. What we now need is to show that each partition results from exactly one such shuffle.

Suppose we have a partition with k parts. If a shuffle leaves the deck sorted, the last entry, m_n, must be 1. If the part containing n is A_1, then it must be that $m_i = 1$ if and only if $i \in A_1$. If $k = 1$, then the only part contains all of $\{1, 2, \ldots, n\}$, and the shuffle must be $(1, 1, 1, \ldots, 1)$.

If $k > 1$, the last move that is not 1 must be 2, since 2 must end up immediately after 1. Thus, if j_2 is the largest index such that $j_2 \notin A_1$, let A_2 be the part containing j_2, and it must be that $m_i = 2$ if and only if $i \in A_2$. We continue in this way: Once we have discovered which of the m_i must have values $1, 2, \ldots, p$, let j_{p+1} be the largest index such that $j_{p+1} \notin A_1 \cup \cdots \cup A_p$, let A_{p+1} be the part containing j_{p+1}, and then $m_i = p + 1$ if and only if $i \in A_{p+1}$. When $p = k$, all values m_i have been determined, and this is the unique shuffle that corresponds to the partition. ■

EXAMPLE 1.4.8 Consider the partition $\{\{1, 5\}, \{2, 3, 6\}, \{4, 7\}\}$. We must have $m_7 = m_4 = 1$, $m_6 = m_3 = m_2 = 2$, and $m_5 = m_1 = 3$, so the shuffle is $(3, 2, 2, 1, 3, 2, 1)$. □

Returning to the problem of writing a computer program to generate a partition: is this a good method? When we say we want a random permutation, we mean that we want each permutation to occur with equal probability, namely, $1/n!$. Since the original order is one of the permutations, we want the number of shuffles that produce it to be exactly $n^n/n!$, but $n!$ does not divide n^n, so this is impossible. The probability of getting

the original permutation is B_n/n^n, and this turns out to be quite a bit larger than $1/n!$. Thus, this is not a suitable method for generating random permutations.

The recurrence relation above is a somewhat cumbersome way to compute the Bell numbers. Another way to compute them is with a different recurrence, expressed in the Bell triangle, whose construction is similar to that of Pascal's triangle:

$A_{1,1}$				1			
$A_{2,1}$	$A_{2,2}$			1	2		
$A_{3,1}$	$A_{3,2}$	$A_{3,3}$		2	3	5	
$A_{4,1}$	$A_{4,2}$	$A_{4,3}$	$A_{4,4}$	5	7	10	15

The rule for constructing this triangle is: $A_{1,1} = 1$; the first entry in each row is the last entry in the previous row; other entries are $A_{n,k} = A_{n,k-1} + A_{n-1,k-1}$; row n has n entries. Both the first column and the diagonal consist of the Bell numbers, with $A_{n,1} = B_{n-1}$ and $A_{n,n} = B_n$.

$A_{n,k}$ may be interpreted as the number of partitions of $\{1, 2, \ldots, n+1\}$ in which $\{k+1\}$ is the singleton set with the largest entry in the partition. For example, $A_{3,2} = 3$; the partitions of $3+1 = 4$ in which $2+1 = 3$ is the largest number appearing in a singleton set are $\{\{1\}, \{2, 4\}, \{3\}\}$, $\{\{2\}, \{1, 4\}, \{3\}\}$, and $\{\{1, 2, 4\}, \{3\}\}$.

To see that this indeed works as advertised, we need to confirm a few things. First, consider $A_{n,n}$, the number of partitions of $\{1, 2, \ldots, n+1\}$ in which $\{n+1\}$ is the singleton set with the largest entry in the partition. Since $n + 1$ is the largest element of the set, all partitions containing the singleton $\{n + 1\}$ satisfy the requirement, and so the B_n partitions of $\{1, 2, \ldots, n\}$ together with $\{n+1\}$ are exactly the partitions of interest, that is, $A_{n,n} = B_n$.

Next, we verify that under the desired interpretation, it is indeed true that $A_{n,k} = A_{n,k-1} + A_{n-1,k-1}$ for $k > 1$. Consider a partition counted by $A_{n,k-1}$. This contains the singleton $\{k\}$, and the element $k + 1$ is not in a singleton. If we interchange k and $k + 1$, we get the singleton $\{k + 1\}$, and no larger element is in a singleton. This gives us partitions in which $\{k + 1\}$ is a singleton and $\{k\}$ is not. Now consider a partition of $\{1, 2, \ldots, n\}$ counted by $A_{n-1,k-1}$. Replace all numbers $j > k$ by $j + 1$, and add the singleton $\{k + 1\}$. This produces a partition in which both $\{k + 1\}$ and $\{k\}$ appear. In fact, we have described how to produce each partition counted by $A_{n,k}$ exactly once, and so $A_{n,k} = A_{n,k-1} + A_{n-1,k-1}$.

Finally, we need to verify that $A_{n,1} = B_{n-1}$; we establish a bijection between the two sets. Suppose a partition in $A_{n,1}$ has the form $\{\{1\}, \{2\}, X_1, X_2, \ldots, X_k\}$, where no X_i is a singleton. Then the collection $\{X_1, X_2, \ldots, X_k\}$ is a partition of the $n - 1$ element set $\{3, 4, \ldots, n + 1\}$. Now we subtract 2 from every element to get a partition of $[n - 1]$ that has no singleton sets. Any other partition in $A_{n,1}$ has the form $\{\{2\}, X_1, X_2, \ldots, X_k\}$, where no X_i is a singleton. One of the sets X_i contains $n+1$, say X_1.

Remove $n+1$ and split the remainder of X_1 into singleton sets $\{x_1\}, \{x_2\}, \ldots, \{x_m\}$. Now $\{\{x_1\}, \{x_2\}, \ldots, \{x_m\}, X_2, X_3, \ldots, X_k\}$ is a partition of the $n-1$ element set $\{1, 3, \ldots, n\}$. Subtracting one from all the elements except 1 produces a partition of $[n-1]$ with at least one singleton set. If $p \in A_{n,1}$, designate the partition of $[n-1]$ obtained in this way by $f(p)$.

Now we define a function g from B_{n-1} to $A_{n,1}$. If partition $p \in B_{n-1}$ contains no singletons, say $p = \{X_1, \ldots, X_k\}$, add two to every element forming sets X_i^*, and let $g(p) = \{\{1\}, \{2\}, X_1^*, \ldots, X_k^*\}$. If p contains singletons, say $p = \{\{x_1\}, \{x_2\}, \ldots, \{x_m\}, X_2, X_3, \ldots, X_k\}$, then add 1 to all elements except 1, forming a partition $\{\{x_1^*\}, \{x_2^*\}, \ldots, \{x_m^*\}, X_2^*, X_3^*, \ldots, X_k^*\}$ of the set $\{1, 3, \ldots, n\}$. Now let $g(p) = \{\{2\}, \{x_1^*, x_2^*, \ldots, x_m^*, n+1\}, X_2^*, \ldots, X_k^*\}$.

Since $f(g(p)) = p$ and $g(f(p)) = p$, f and g are inverses and so f is a bijection between $A_{n,1}$ and B_{n-1}, as desired.

Exercises 1.4.

1. Show that if $\{A_1, A_2, \ldots, A_k\}$ is a partition of $\{1, 2, \ldots, n\}$, then there is a unique equivalence relation $\equiv$ whose equivalence classes are $\{A_1, A_2, \ldots, A_k\}$.

2. Suppose n is a square-free number, that is, no number m^2 divides n; put another way, square-free numbers are products of distinct prime factors, that is, $n = p_1 p_2 \cdots p_k$, where each p_i is prime and no two prime factors are equal. Find the number of factorizations of n. For example, $30 = 2 \cdot 3 \cdot 5$, and the factorizations of 30 are 30, $6 \cdot 5$, $10 \cdot 3$, $2 \cdot 15$, and $2 \cdot 3 \cdot 5$. Note we count 30 alone as a factorization, though in some sense a trivial factorization.

3. The rhyme scheme of a stanza of poetry indicates which lines rhyme. This is usually expressed in the form ABAB, meaning the first and third lines of a four line stanza rhyme, as do the second and fourth, or ABCB, meaning only lines two and four rhyme, and so on. A limerick is a five line poem with rhyming scheme AABBA. How many different rhyme schemes are possible for an n line stanza? To avoid duplicate patterns, we only allow a new letter into the pattern when all previous letters have been used to the left of the new one. For example, ACBA is not allowed, since when C is placed in position 2, B has not been used to the left. This is the same rhyme scheme as ABCA, which is allowed.

4. Another way to express the Bell numbers for $n > 0$ is

$$B_n = \sum_{k=1}^{n} S(n, k),$$

where $S(n, k)$ is the number of partitions of $\{1, 2, \ldots, n\}$ into exactly k parts, $1 \le k \le n$. The $S(n, k)$ are the **Stirling numbers of the second kind**. Find a recurrence relation for $S(n, k)$. Your recurrence should allow a fairly simple triangle construction containing the values $S(n, k)$, and then the Bell numbers may be computed by summing the rows of this triangle. Show the first five rows of the triangle, $n \in \{1, 2, \ldots, 5\}$.

5. Let A_n be the number of partitions of $\{1, 2, \ldots, n+1\}$ in which no consecutive integers are in the same part of the partition. For example, when $n = 3$ these partitions are $\{\{1\}, \{2\}, \{3\}, \{4\}\}$, $\{\{1\}, \{2, 4\}, \{3\}\}$, $\{\{1, 3\}, \{2\}, \{4\}\}$, $\{\{1, 3\}, \{2, 4\}\}$, $\{\{1, 4\}, \{2\}, \{3\}\}$, so $A_3 = 5$. Let $A(n, k)$ be the number of partitions of $\{1, 2, \ldots, n+1\}$ into exactly k parts,

in which no consecutive integers are in the same part of the partition. Thus

$$A_n = \sum_{k=2}^{n+1} A(n,k).$$

Find a recurrence for $A(n,k)$ and then show that $A_n = B_n$.

1.5 Choice with repetition

Most of the permutation and combination problems we have seen count choices made without repetition, as when we asked how many rolls of three dice are there in which each die has a different value. The exception was the simplest problem, asking for the total number of outcomes when two or three dice are rolled, a simple application of the multiplication principle. Typical permutation and combination problems can be interpreted in terms of drawing balls from a box, and implicitly or explicitly the rule is that a ball drawn from the box stays out of the box. If instead each ball is returned to the box after recording the draw, we get a problem essentially identical to the general dice problem. For example, if there are six balls, numbered 1–6, and we draw three balls with replacement, the number of possible outcomes is 6^3. Another version of the problem does not replace the ball after each draw, but allows multiple "identical" balls to be in the box. For example, if a box contains 18 balls numbered 1–6, three with each number, then the possible outcomes when three balls are drawn and not returned to the box is again 6^3. If four balls are drawn, however, the problem becomes different.

Another, perhaps more mathematical, way to phrase such problems is to introduce the idea of a **multiset**. A multiset is like a set, except that elements may appear more than once. If $\{a,b\}$ and $\{b,c\}$ are ordinary sets, we say that the union $\{a,b\} \cup \{b,c\}$ is $\{a,b,c\}$, not $\{a,b,b,c\}$. If we interpret these as multisets, however, we do write $\{a,b,b,c\}$ and consider this to be different than $\{a,b,c\}$. To distinguish multisets from sets, and to shorten the expression in most cases, we use a **repetition number** with each element. For example, we will write $\{a,b,b,c\}$ as $\{1\cdot a, 2\cdot b, 1\cdot c\}$. By writing $\{1\cdot a, 1\cdot b, 1\cdot c\}$ we emphasize that this is a multiset, even though no element appears more than once. We also allow elements to be included an infinite number of times, indicated with ∞ for the repetition number, like $\{\infty\cdot a, 5\cdot b, 3\cdot c\}$.

Generally speaking, problems in which repetition numbers are infinite are easier than those involving finite repetition numbers. Given a multiset $A = \{\infty\cdot a_1, \infty\cdot a_2, \ldots, \infty\cdot a_n\}$, how many permutations of the elements of length k are there? That is, how many sequences $x_1, x_2, \ldots, x_k$ can be formed? This is easy: the answer is n^k.

Now consider combinations of a multiset, that is, submultisets: Given a multiset, how many submultisets of a given size does it have? We say that a multiset A is a submultiset of B if the repetition number of every element of A is less than or equal to its repetition

number in B. For example, $\{20 \cdot a, 5 \cdot b, 1 \cdot c\}$ is a submultiset of $\{\infty \cdot a, 5 \cdot b, 3 \cdot c\}$. A multiset is finite if it contains only a finite number of distinct elements, and the repetition numbers are all finite. Suppose again that $A = \{\infty \cdot a_1, \infty \cdot a_2, \ldots, \infty \cdot a_n\}$; how many finite submultisets does it have of size k? This at first seems quite difficult, but put in the proper form it turns out to be a familiar problem. Imagine that we have $k + n - 1$ "blank spaces", like this:

$$\_ \ \_ \ \_ \ \_ \ \_ \ \_ \ \_ \ \_ \ \cdots \ \_ \ \_ \ \_ \ \_$$

Now we place $n - 1$ markers in some of these spots:

$$\underline{\wedge} \ \_ \ \underline{\wedge} \ \_ \ \_ \ \_ \ \underline{\wedge} \ \_ \ \cdots \ \_ \ \_ \ \underline{\wedge} \ \_$$

This uniquely identifies a submultiset: fill all blanks up to the first $\wedge$ with a_1, up to the second with a_2, and so on:

$$\underline{\wedge} \ \underline{a_2} \ \underline{\wedge} \ \underline{a_3} \ \underline{a_3} \ \underline{a_3} \ \underline{\wedge} \ \underline{a_4} \ \ldots \ \underline{a_{n-1}} \ \underline{a_{n-1}} \ \underline{\wedge} \ \underline{a_n}$$

So this pattern corresponds to the multiset $\{1 \cdot a_2, 3 \cdot a_3, \ldots, 1 \cdot a_n\}$. Filling in the markers $\wedge$ in all possible ways produces all possible submultisets of size k, so there are $\binom{k+n-1}{n-1}$ such submultisets. Note that this is the same as $\binom{k+n-1}{k}$; the hard part in practice is remembering that the -1 goes with the n, not the k.

• • •

Summarizing the high points so far: The number of permutations of n things taken k at a time without replacement is $P(n, k) = n!/(n - k)!$; the number of permutations of n things taken k at a time with replacement is n^k. The number of combinations of n things taken k at a time without replacement is $\binom{n}{k}$; the number of combinations of n things taken k at a time with replacement is $\binom{k+n-1}{k}$.

• • •

If $A = \{m_1 \cdot a_1, m_2 \cdot a_2, \ldots, m_n \cdot a_n\}$, similar questions can be quite hard. Here is an easier special case: How many permutations of the multiset A are there? That is, how many sequences consist of m_1 copies of a_1, m_1 copies of a_2, and so on? This problem succumbs to overcounting: suppose to begin with that we can distinguish among the different copies of each a_i; they might be colored differently for example: a red a_1, a blue a_1, and so on. Then we have an ordinary set with $M = \sum_{i=1}^{n} m_i$ elements and $M!$ permutations. Now if we ignore the colors, so that all copies of a_i look the same, we find that we have overcounted the desired permutations. Permutations with, say, the a_1 items in the same positions all look the same once we ignore the colors of the a_1s. How many of the original permutations have this property? $m_1!$ permutations will appear identical once we ignore

the colors of the a_1 items, since there are $m_1!$ permutations of the colored a_1s in a given m_1 positions. So after throwing out duplicates, the number of remaining permutations is $M!/m_1!$ (assuming the other a_i are still distinguishable). Then the same argument applies to the a_2s: there are $m_2!$ copies of each permutation once we ignore the colors of the a_2s, so there are $\dfrac{M!}{m_1!\,m_2!}$ distinct permutations. Continuing in this way, we see that the number of distinct permutations once all colors are ignored is

$$\frac{M!}{m_1!\,m_2!\cdots m_n!}.$$

This is frequently written

$$\binom{M}{m_1\ \ m_2\ \ \ldots\ m_n},$$

called a **multinomial coefficient**. Here the second row has n separate entries, not a single product entry. Note that if $n = 2$ this is

$$\binom{M}{m1\ \ m2} = \frac{M!}{m_1!\,m_2!} = \frac{M!}{m_1!\,(M-m_1)!} = \binom{M}{m_1}. \tag{1.5.1}$$

This is easy to see combinatorially: given $\{m_1 \cdot a_1, m_2 \cdot a_2\}$ we can form a permutation by choosing the m_1 places that will be occupied by a_1, filling in the remaining m_2 places with a_2. The number of permutations is the number of ways to choose the m_1 locations, which is $\binom{M}{m_1}$.

EXAMPLE 1.5.1 How many solutions does $x_1+x_2+x_3+x_4 = 20$ have in non-negative integers? That is, how many 4-tuples (m_1, m_2, m_3, m_4) of non-negative integers are solutions to the equation? We have actually solved this problem: How many submultisets of size 20 are there of the multiset $\{\infty \cdot a_1, \infty \cdot a_2, \infty \cdot a_3, \infty \cdot a_4\}$? A submultiset of size 20 is of the form $\{m_1 \cdot a_1, m_2 \cdot a_2, m_3 \cdot a_3, m_4 \cdot a_4\}$ where $\sum m_i = 20$, and these are in 1–1 correspondence with the set of 4-tuples (m_1, m_2, m_3, m_4) of non-negative integers such that $\sum m_i = 20$. Thus, the number of solutions is $\binom{20+4-1}{20}$. This reasoning applies in general: the number of solutions to

$$\sum_{i=1}^{n} x_i = k$$

is

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

□

This immediately suggests some generalizations: instead of the total number of solutions, we might want the number of solutions with the variables x_i in certain ranges, that is, we might require that $m_i \le x_i \le M_i$ for some lower and upper bounds m_i and M_i.

Finite upper bounds can be difficult to deal with; if we require that $0 \le x_i \le M_i$, this is the same as counting the submultisets of $\{M_1 \cdot a_1, M_2 \cdot a_2, \ldots, M_n \cdot a_n\}$. Lower bounds are easier to deal with.

EXAMPLE 1.5.2 Find the number of solutions to $x_1 + x_2 + x_3 + x_4 = 20$ with $x_1 \ge 0$, $x_2 \ge 1$, $x_3 \ge 2$, $x_4 \ge -1$.

We can transform this to the initial problem in which all lower bounds are 0. The solutions we seek to count are the solutions of this altered equation:

$$x_1 + (x_2 - 1) + (x_3 - 2) + (x_4 + 1) = 18.$$

If we set $y_1 = x_1$, $y_2 = x_2 - 1$, $y_3 = x_3 - 2$, and $y_4 = x_4 + 1$, then (x_1, x_2, x_3, x_4) is a solution to this equation if and only if (y_1, y_2, y_3, y_4) is a solution to

$$y_1 + y_2 + y_3 + y_4 = 18,$$

and moreover the bounds on the x_i are satisfied if and only if $y_i \ge 0$. Since the number of solutions to the last equation is $\binom{18+4-1}{18}$, this is also the number of solutions to the original equation. □

Exercises 1.5.

1. Suppose a box contains 18 balls numbered 1–6, three balls with each number. When 4 balls are drawn without replacement, how many outcomes are possible? Do this in two ways: assuming that the order in which the balls are drawn matters, and then assuming that order does not matter.
2. How many permutations are there of the letters in Mississippi?
3. How many permutations are there of the multiset $\{1 \cdot a_1, 1 \cdot a_2, \ldots, 1 \cdot a_n\}$?
4. Let $M = \sum_{i=1}^{n} m_i$. If $k_i < 0$ for some i, let's say

$$\binom{M}{k_1\ k_2\ \ldots\ k_n} = 0.$$

Prove that

$$\binom{M}{m_1\ m_2\ \ldots\ m_n} = \sum_{i=1}^{n} \binom{M-1}{m_1\ m_2\ \ldots\ (m_i - 1)\ \ldots\ m_n}.$$

Note that when $n = 2$ this becomes

$$\binom{M}{m_1\ m_2} = \binom{M-1}{(m_1 - 1)\ m_2} + \binom{M-1}{m_1\ (m_2 - 1)}.$$

As noted above in equation 1.5.1, when $n = 2$ we are really seeing ordinary binomial coefficients, and this can be rewritten as

$$\binom{M}{m_1} = \binom{M-1}{m_1 - 1} + \binom{M-1}{m_1},$$

which of course we already know.

5. The Binomial Theorem (1.3.1) can be written

$$(x+y)^n = \sum_{i+j=n} \binom{n}{i\ j} x^i\, y^j,$$

where the sum is over all non-negative integers i and j that sum to n. Prove that for $m \geq 2$,

$$(x_1 + x_2 + \cdots + x_m)^n = \sum \binom{n}{i_1\ i_2\ \ldots\ i_m} x_1^{i_1}\, x_2^{i_2} \ldots x_m^{i_m}.$$

where the sum is over all $i_1, \ldots, i_m$ such that $i_1 + \cdots + i_m = n$.

6. Find the number of integer solutions to

$$x_1 + x_2 + x_3 + x_4 + x_5 = 50, x_1 \geq -3, x_2 \geq 0, x_3 \geq 4, x_4 \geq 2, x_5 \geq 12.$$

7. You and your spouse each take two gummy vitamins every day. You share a single bottle of 60 vitamins, 30 of one flavor and 30 of another. You each prefer a different flavor, but it seems childish to fish out two of each type (but not to take gummy vitamins). So you just take the first four that fall out and then divide them up according to your preferences. For example, if there are two of each flavor, you and your spouse get the vitamins you prefer, but if three of your preferred flavor come out, you get two of the ones you like and your spouse gets one of each. Of course, you start a new bottle every 15 days. On average, over a 15 day period, how many of the vitamins you take are the flavor you prefer? (From fivethirtyeight.com.)

1.6 The Pigeonhole Principle

A key step in many proofs consists of showing that two possibly different values are in fact the same. The **Pigeonhole principle** can sometimes help with this.

THEOREM 1.6.1 Pigeonhole Principle Suppose that $n+1$ (or more) objects are put into n boxes. Then some box contains at least two objects.

Proof. Suppose each box contains at most one object. Then the total number of objects is at most $1 + 1 + \cdots + 1 = n$, a contradiction. ■

This seemingly simple fact can be used in surprising ways. The key typically is to put objects into boxes according to some rule, so that when two objects end up in the same box it is because they have some desired relationship.

EXAMPLE 1.6.2 Among any 13 people, at least two share a birth month.

Label 12 boxes with the names of the months. Put each person in the box labeled with his or her birth month. Some box will contain at least two people, who share a birth month. □

EXAMPLE 1.6.3 Suppose 5 pairs of socks are in a drawer. Picking 6 socks guarantees that at least one pair is chosen.

Label the boxes by "the pairs" (e.g., the red pair, the blue pair, the argyle pair,...). Put the 6 socks into the boxes according to description. □

Some uses of the principle are not nearly so straightforward.

EXAMPLE 1.6.4 Suppose $a_1, \ldots, a_n$ are integers. Then some "consecutive sum" $a_k + a_{k+1} + a_{k+2} + \cdots + a_{k+m}$ is divisible by n.

Consider these n sums:

$$\begin{aligned} s_1 &= a_1 \\ s_2 &= a_1 + a_2 \\ s_3 &= a_1 + a_2 + a_3 \\ &\vdots \\ s_n &= a_1 + a_2 + \cdots + a_n \end{aligned}$$

These are all consecutive sums, so if one of them is divisible by n we are done. If not, dividing each by n leaves a non-zero remainder, $r_1 = s_1 \bmod n$, $r_2 = s_2 \bmod n$, and so on. These remainders have values in $\{1, 2, 3, \ldots, n-1\}$. Label $n-1$ boxes with these $n-1$ values; put each of the n sums into the box labeled with its remainder mod n. Two sums end up in the same box, meaning that $s_i \bmod n = s_j \bmod n$ for some $j > i$; hence $s_j - s_i$ is divisible by n, and $s_j - s_i = a_{i+1} + a_{i+2} + \cdots + a_j$, as desired. □

A similar argument provides a proof of the **Chinese Remainder Theorem**.

THEOREM 1.6.5 Chinese Remainder Theorem If m and n are relatively prime, and $0 \le a < m$ and $0 \le b < n$, then there is an integer x such that $x \bmod m = a$ and $x \bmod n = b$.

Proof. Consider the integers $a, a+m, a+2m, \ldots a+(n-1)m$, each with remainder a when divided by m. We wish to show that one of these integers has remainder b when divided by n, in which case that number satisfies the desired property.

For a contradiction, suppose not. Let the remainders be $r_0 = a \bmod n$, $r_1 = a+m \bmod n$,..., $r_{n-1} = a + (n-1)m \bmod n$. Label $n-1$ boxes with the numbers $0, 1, 2, 3, \ldots, b-1, b+1, \ldots n-1$. Put each r_i into the box labeled with its value. Two remainders end up in the same box, say r_i and r_j, with $j > i$, so $r_i = r_j = r$. This means that

$$a + im = q_1 n + r \quad \text{and} \quad a + jm = q_2 n + r.$$

Hence

$$\begin{aligned} a + jm - (a + im) &= q_2 n + r - (q_1 n + r) \\ (j - i)m &= (q_2 - q_1)n. \end{aligned}$$

Since n is relatively prime to m, this means that $n \mid (j-i)$. But since i and j are distinct and in $\{0, 1, 2, \ldots, n-1\}$, $0 < j - i < n$, so $n \nmid (j-i)$. This contradiction finishes the proof. ■

More general versions of the Pigeonhole Principle can be proved by essentially the same method. A natural generalization would be something like this: *If X objects are put into n boxes, some box contains at least m objects.* For example:

THEOREM 1.6.6 Suppose that $r_1, \ldots, r_n$ are positive integers. If $X \geq (\sum_{i=1}^{n} r_i) - n + 1$ objects are put into n boxes labeled $1, 2, 3, \ldots, n$, then some box labeled i contains at least r_i objects.

Proof. Suppose not. Then the total number of objects in the boxes is at most $(r_1 - 1) + (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1) = (\sum_{i=1}^{n} r_i) - n < X$, a contradiction. ■

This full generalization is only occasionally needed; often this simpler version is sufficient:

COROLLARY 1.6.7 Suppose $r > 0$ and $X \geq n(r-1) + 1$ objects are placed into n boxes. Then some box contains at least r objects.

Proof. Apply the previous theorem with $r_i = r$ for all i. ■

• • •

Here is a simple application of the Pigeonhole Principle that leads to many interesting questions.

EXAMPLE 1.6.8 Suppose 6 people are gathered together; then either 3 of them are mutually acquainted, or 3 of them are mutually unacquainted.

We turn this into a graph theory question: Consider the graph consisting of 6 vertices, each connected to all the others by an edge, called the **complete graph** on 6 vertices, and denoted K_6; the vertices represent the people. Color an edge red if the people represented by its endpoints are acquainted, and blue if they are not acquainted. Any choice of 3 vertices defines a triangle; we wish to show that either there is a red triangle or a blue triangle.

Consider the five edges incident at a single vertex v; by the Pigeonhole Principle (the version in corollary 1.6.7, with $r = 3$, $X = 2(3-1) + 1 = 5$), at least three of them are the same color, call it color C; call the other color D. Let the vertices at the other ends of these three edges be v_1, v_2, v_3. If any of the edges between these vertices have color C, there is a triangle of color C: if the edge connects v_i to v_j, the triangle is formed by v,

v_i, and v_j. If this is not the case, then the three vertices v_1, v_2, v_3 are joined by edges of color D, and form a triangle of color D. □

The number 6 in this example is special: with 5 or fewer vertices it is not true that there must be a monochromatic triangle, and with more than 6 vertices it is true. To see that it is not true for 5 vertices, we need only show an example, as in figure 1.6.1.

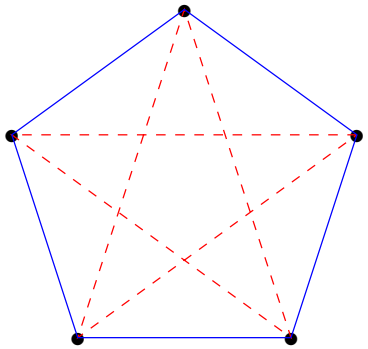


Figure 1.6.1 An edge coloring with no monochromatic triangles.

The **Ramsey number** $R(i)$ is the smallest integer n such that when the edges of K_n are colored with two colors, there is a monochromatic complete graph on i vertices, K_i, contained within K_n. The example shows that $R(3) = 6$.

More generally, $R(i, j)$ is the smallest integer n such that when the edges of K_n are colored with two colors, say C_1 and C_2, either there is a K_i contained within K_n all of whose edges are color C_1, or there is a K_j contained within K_n all of whose edges are color C_2. Using this notion, $R(k) = R(k, k)$. More generally still, $R(i_1, i_2, \ldots, i_m)$ is the smallest integer n such that when the edges of K_n are colored with m colors, $C_1, \ldots, C_m$, then for some j there is a K_{i_j} contained in K_n all of whose edges are color C_j.

Ramsey proved that in all of these cases, there actually is such a number n. Generalizations of this problem have led to the subject called **Ramsey Theory**.

Computing any particular value $R(i, j)$ turns out to be quite difficult; Ramsey numbers are known only for a few small values of i and j, and in some other cases the Ramsey number is bounded by known numbers. Typically in these cases someone has exhibited a K_m and a coloring of the edges without the existence of a monochromatic K_i or K_j of the desired color, showing that $R(i, j) > m$; and someone has shown that whenever the edges of K_n have been colored, there is a K_i or K_j of the correct color, showing that $R(i, j) \leq n$.

Exercises 1.6.

1. Assume that the relation "friend" is symmetric. Show that if $n \geq 2$, then in any group of n people there are two with the same number of friends in the group.

2. Suppose that 501 distinct integers are selected from $1 \ldots 1000$. Show that there are distinct selected integers a and b such that $a \mid b$. Show that this is not always true if 500 integers are selected. ⇒

3. Each of 15 red balls and 15 green balls is marked with an integer between 1 and 100 inclusive; no integer appears on more than one ball. The value of a pair of balls is the sum of the numbers on the balls. Show there are at least two pairs, consisting of one red and one green ball, with the same value. Show that this is not necessarily true if there are 13 balls of each color.

4. Suppose we have 14 red balls and 14 green balls as in the previous exercise. Show that at least two pairs, consisting of one red and one green ball, have the same value. What about 13 red balls and 14 green balls?

5. Suppose $(a_1, a_2, \ldots, a_{52})$ are integers, not necessarily distinct. Show that there are two, a_i and a_j with $i \neq j$, such that either $a_i + a_j$ or $a_i - a_j$ is divisible by 100. Show that this is not necessarily true for integers $(a_1, a_2, \ldots, a_{51})$.

6. Suppose five points are chosen from a square whose sides are length s. (The points may be either in the interior of the square or on the boundary.) Show that two of the points are at most $s\sqrt{2}/2$ apart. Find five points so that no two are less than $s\sqrt{2}/2$ apart.

7. Show that if the edges of K_6 are colored with two colors, there are at least two monochromatic triangles. (Two triangles are different if each contains at least one vertex not in the other. For example, two red triangles that share an edge count as two triangles.) Color the edges of K_6 so that there are exactly two monochromatic triangles.

8. Suppose the edges of a K_5 are colored with two colors, say red and blue, so that there are no monochromatic triangles. Show that the red edges form a cycle, and the blue edges form a cycle, each with five edges. (A **cycle** is a sequence of edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_k, v_1\}$, where all of the v_i are distinct. Note that this is true in figure 1.6.1.)

9. Show that $8 < R(3, 4) \leq 10$.

10. Show that $R(3, 4) = 9$.

1.7 Sperner's Theorem

The binomial coefficients count the subsets of a given set; the sets themselves are worth looking at. First some convenient notation:

DEFINITION 1.7.1 Let $[n] = \{1, 2, 3, \ldots, n\}$. Then $2^{[n]}$ denotes the set of all subsets of $[n]$, and $\begin{bmatrix} n \\ k \end{bmatrix}$ denotes the set of subsets of $[n]$ of size k. □

EXAMPLE 1.7.2 Let $n = 3$. Then

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \{\emptyset\}$$
$$\begin{bmatrix} n \\ 1 \end{bmatrix} = \{\{1\}, \{2\}, \{3\}\}$$
$$\begin{bmatrix} n \\ 2 \end{bmatrix} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$$
$$\begin{bmatrix} n \\ 3 \end{bmatrix} = \{\{1, 2, 3\}\}$$

□

DEFINITION 1.7.3 A **chain** in $2^{[n]}$ is a set of subsets of $2^{[n]}$ that are linearly ordered by inclusion. An **anti-chain** in $2^{[n]}$ is a set of subsets of $2^{[n]}$ that are pairwise incomparable. □

EXAMPLE 1.7.4 In $2^{[3]}$, $\{\emptyset, \{1\}, \{1,2,3\}\}$ is a chain, because $\emptyset \subseteq \{1\} \subseteq \{1,2,3\}$. Every $\begin{bmatrix} n \\ k \end{bmatrix}$ is an anti-chain, as is $\{\{1\}, \{2,3\}\}$. The set $\{\{1\}, \{1,3\}, \{2,3\}\}$ is neither a chain nor an anti-chain. □

Because of theorem 1.3.4 we know that among all anti-chains of the form $\begin{bmatrix} n \\ k \end{bmatrix}$ the largest are the "middle" ones, namely $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$ and $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$ (which are the same if n is even). Remarkably, these are the largest of all anti-chains, that is, strictly larger than every other anti-chain. When $n = 3$, the anti-chains $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$ are the only anti-chains of size 3, and no anti-chain is larger, as you can verify by examining all possibilities.

Before we prove this, a bit of notation.

DEFINITION 1.7.5 If $\sigma: A \to A$ is a bijection, then σ is called a permutation. □

This use of the word permutation is different than our previous usage, but the two are closely related. Consider such a function $\sigma: [n] \to [n]$. Since the set A in this case is finite, we could in principle list every value of σ:

$$\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n).$$

This is a list of the numbers $\{1, \ldots, n\}$ in some order, namely, this is a permutation according to our previous usage. We can continue to use the same word for both ideas, relying on context or an explicit statement to indicate which we mean.

THEOREM 1.7.6 (Sperner's Theorem) The only anti-chains of largest size are $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$ and $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$.

Proof. First we show that no anti-chain is larger than these two. We attempt to partition $2^{[n]}$ into $k = \binom{n}{\lfloor n/2 \rfloor}$ chains, that is, to find chains

$$\begin{aligned}
&A_{1,0} \subseteq A_{1,1} \subseteq A_{1,2} \subseteq \cdots \subseteq A_{1,m_1} \\
&A_{2,0} \subseteq A_{2,1} \subseteq A_{2,2} \subseteq \cdots \subseteq A_{2,m_2} \\
&\vdots \\
&A_{k,0} \subseteq A_{k,1} \subseteq A_{k,2} \subseteq \cdots \subseteq A_{k,m_k}
\end{aligned}$$

so that every subset of $[n]$ appears exactly once as one of the $A_{i,j}$. If we can find such a partition, then since no two elements of an anti-chain can be in the same chain, no anti-chain can have more than k elements.

For small values of n this can be done by hand; for $n = 3$ we have

$$\emptyset \subseteq \{1\} \subseteq \{1,2\} \subseteq \{1,2,3\}$$
$$\{2\} \subseteq \{2,3\}$$
$$\{3\} \subseteq \{1,3\}$$

These small cases form the base of an induction. We will prove that any $2^{[n]}$ can be partitioned into such chains with two additional properties:

1. Each set in a chain contains exactly one element more than the next smallest set in the chain.
2. The sum of the sizes of the smallest and largest element in the chain is n.

Note that the chains for the case $n = 3$ have both of these properties. The two properties taken together imply that every chain "crosses the middle", that is, every chain contains an element of $\binom{n}{n/2}$ if n is even, and an element of both $\binom{n}{\lfloor n/2 \rfloor}$ and $\binom{n}{\lceil n/2 \rceil}$ if n is odd. Thus, if we succeed in showing that such chain partitions exist, there will be exactly $\binom{n}{\lfloor n/2 \rfloor}$ chains.

For the induction step, we assume that we have partitioned $2^{[n-1]}$ into such chains, and construct chains for $2^{[n]}$.

First, for each chain $A_{i,0} \subseteq A_{i,1} \subseteq \cdots \subseteq A_{i,m_i}$ we form a new chain $A_{i,0} \subseteq A_{i,1} \subseteq \cdots \subseteq A_{i,m_i} \subseteq A_{i,m_i} \cup \{n\}$. Since $|A_{i,0}| + |A_{i,m_i}| = n - 1$, $|A_{i,0}| + |A_{i,m_i} \cup \{n\}| = n$, so this new chain satisfies properties (1) and (2).

In addition, if $m_i > 0$, we form a new chain $A_{i,0} \cup \{n\} \subseteq A_{i,1} \cup \{n\} \subseteq \cdots \subseteq A_{i,m_i-1} \cup \{n\}$. Now

$$\begin{aligned} |A_{i,0} \cup \{n\}| + |A_{i,m_i-1} \cup \{n\}| &= |A_{i,0}| + 1 + |A_{i,m_i-1}| + 1 \\ &= |A_{i,0}| + 1 + |A_{i,m_i}| - 1 + 1 \\ &= n - 1 + 1 = n \end{aligned}$$

so again properties (1) and (2) are satisfied.

Because of the first type of chain, all subsets of $[n-1]$ are contained exactly once in the new set of chains. Also, we have added the element n exactly once to every subset of $[n-1]$, so we have included every subset of $[n]$ containing n exactly once. Thus we have produced the desired partition of $2^{[n]}$.

Now we need to show that the only largest anti-chains are $\binom{n}{\lfloor n/2 \rfloor}$ and $\binom{n}{\lceil n/2 \rceil}$.

Suppose that $A_1, A_2, \ldots, A_m$ is an anti-chain; then $A_1^c, A_2^c, \ldots, A_m^c$ is also an anti-chain, where A^c denotes the complement of A. Thus, if there is an anti-chain that contains some A with $|A| > \lceil n/2 \rceil$, there is also one containing A^c, and $|A^c| < \lfloor n/2 \rfloor$. Suppose that some

anti-chain contains a set A with $|A| < \lfloor n/2 \rfloor$. We next prove that this anti-chain cannot be of maximum size.

Partition $2^{[n]}$ as in the first part of the proof. Suppose that A is a subset of the elements of a one or two element chain C, that is, a chain consisting solely of a set S_1 of size $n/2$, if n is even, or of sets S_1 and S_2 of sizes $\lfloor n/2 \rfloor$ and $\lceil n/2 \rceil$, with $A \subseteq S_1 \subseteq S_2$, if n is odd. Then no member of C is in the anti-chain. Thus, the largest possible size for an anti-chain containing A is $\binom{n}{\lfloor n/2 \rfloor} - 1$.

If A is not a subset of the elements of such a short chain, we now prove that there is another chain partition of $2^{[n]}$ that does have this property. Note that in the original chain partition there must be a chain of length 1 or 2, C_1, consisting of S_1 and possibly S_2; if not, every chain would contain a set of size $\lfloor n/2 \rfloor - 1$, but there are not enough such sets to go around. Suppose then that $A = \{x_1, \ldots, x_k\}$ and the set S_1 in C_1 is $S_1 = \{x_1, \ldots, x_q, y_{q+1}, \ldots y_l\}$, where $0 \leq q < k$ and $l > k$.

Let σ be the permutation of $[n]$ such that $\sigma(x_{q+i}) = y_{q+i}$ and $\sigma(y_{q+i}) = x_{q+i}$, for $1 \leq i \leq k - q$, and σ fixes all other elements. Now for $U \subseteq [n]$, let $\overline{U} = \sigma(U)$, and note that $U \subseteq V$ if and only if $\overline{U} \subseteq \overline{V}$. Thus every chain in the original chain partition maps to a chain. Since σ is a bijection, these new chains also form a partition of $2^{[n]}$, with the additional properties (1) and (2). By the definition of σ, $A \subseteq \overline{S}_1$, and $\{\overline{S}_1, \overline{S}_2\}$ is a chain, say $\overline{C}_1$. Thus, this new chain partition has the desired property: A is a subset of every element of the 1 or 2 element chain $\overline{C}_1$, so A is not in an anti-chain of maximum size.

Finally, we need to show that if n is odd, no anti-chain of maximum size contains sets in both $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$ and $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$. Suppose there is such an anti-chain, consisting of sets $A_{k+1}, \ldots, A_l$ in $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$, where $l = \binom{n}{\lceil n/2 \rceil}$, and $B_1, \ldots, B_k$ in $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$. The remaining sets in $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$ are $A_1, \ldots, A_k$, and the remaining sets in $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$ are $B_{k+1}, \ldots, B_l$.

Each set B_i, $1 \leq i \leq k$, is contained in exactly $\lceil n/2 \rceil$ sets in $\begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix}$, and all must be among $A_1, \ldots, A_k$. On average, then, each A_i, $1 \leq i \leq k$, contains $\lceil n/2 \rceil$ sets among $B_1, \ldots, B_k$. But each set A_i, $1 \leq i \leq k$, contains exactly $\lceil n/2 \rceil$ sets in $\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}$, and so each must contain exactly $\lceil n/2 \rceil$ of the sets $B_1, \ldots, B_k$ and none of the sets $B_{k+1}, \ldots, B_l$.

Let $A_1 = A_{j_1} = \{x_1, \ldots, x_r\}$ and $B_{k+1} = \{x_1, \ldots, x_s, y_{s+1}, \ldots, y_{r-1}\}$. Let $B_{i_m} = A_{j_m} \backslash \{x_{s+m}\}$ and $A_{j_{m+1}} = B_{i_m} \cup \{y_{s+m}\}$, for $1 \leq m \leq r-s-1$. Note that by the preceding discussion, $1 \leq i_m \leq k$ and $1 \leq j_m \leq k$. Then $A_{j_{r-s}} = \{x_1, \ldots, x_s, y_{s+1}, \ldots, y_{r-1}, x_r\}$, so $A_{j_{r-s}} \supseteq B_{k+1}$, a contradiction. Hence there is no such anti-chain. ∎

Exercises 1.7.

1. Sperner's Theorem (1.7.6) tells us that $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$, with size 20, is the unique largest anti-chain for $2^{[6]}$. The next largest anti-chains of the form $\begin{bmatrix} 6 \\ k \end{bmatrix}$ are $\begin{bmatrix} 6 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 4 \end{bmatrix}$, with size 15. Find a maximal anti-chain with size larger than 15 but less than 20. (As usual, maximal here means

that the anti-chain cannot be enlarged simply by adding elements. So you may not simply use a subset of $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$.)

1.8 Stirling numbers

In exercise 4 in section 1.4, we saw the Stirling numbers of the second kind. Not surprisingly, there are **Stirling numbers of the first kind**. Recall that Stirling numbers of the second kind are defined as follows:

DEFINITION 1.8.1 The Stirling number of the second kind, $S(n,k)$ or $\left\{ {n \atop k} \right\}$, is the number of partitions of $[n] = \{1, 2, \ldots, n\}$ into exactly k parts, $1 \leq k \leq n$. □

Before we define the Stirling numbers of the first kind, we need to revisit permutations. As we mentioned in section 1.7, we may think of a permutation of $[n]$ either as a reordering of $[n]$ or as a bijection $\sigma\colon [n] \to [n]$. There are different ways to write permutations when thought of as functions. Two typical and useful ways are as a table, and in **cycle form**. Consider this permutation $\sigma\colon [5] \to [5]$: $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 2$, $\sigma(5) = 1$. In table form, we write this as $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{smallmatrix}\right)$, which is somewhat more compact, as we don't write "σ" five times. In cycle form, we write this same permutation as $(1,3,5)(2,4)$. Here $(1,3,5)$ indicates that $\sigma(1) = 3$, $\sigma(3) = 5$, and $\sigma(5) = 1$, whiile $(2,4)$ indicates $\sigma(2) = 4$ and $\sigma(4) = 2$. This permutation has two cycles, a 3-cycle and a 2-cycle. Note that $(1,3,5)$, $(3,5,1)$, and $(5,1,3)$ all mean the same thing. We allow 1-cycles to count as cycles, though sometimes we don't write them explicitly. In some cases, however, it is valuable to write them to force us to remember that they are there. Consider this permutation: $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{smallmatrix}\right)$. If we write this in cycle form as $(1,3,5)(2,4)$, which is correct, there is no indication that the underlying set is really $[6]$. Writing $(1,3,5)(2,4)(6)$ makes this clear. We say that this permutation has 3 cycles, even though one of them is a trivial 1-cycle. Now we're ready for the next definition.

DEFINITION 1.8.2 The **Stirling number of the first kind**, $s(n,k)$, is $(-1)^{n-k}$ times the number of permutations of $[n]$ with exactly k cycles. The corresponding **unsigned Stirling number of the first kind**, the number of permutations of $[n]$ with exactly k cycles, is $|s(n,k)|$, sometimes written $\begin{bmatrix} n \\ k \end{bmatrix}$. Using this notation, $s(n,k) = (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}$. □

Note that the use of $\begin{bmatrix} n \\ k \end{bmatrix}$ conflicts with the use of the same notation in section 1.7; there should be no confusion, as we won't be discussing the two ideas together.

Some values of $\begin{bmatrix} n \\ k \end{bmatrix}$ are easy to see; if $n \geq 1$, then

$$\begin{bmatrix} n \\ n \end{bmatrix} = 1 \qquad \begin{bmatrix} n \\ k \end{bmatrix} = 0, \text{ if } k > n$$
$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)! \qquad \begin{bmatrix} n \\ 0 \end{bmatrix} = 0$$

It is sometimes convenient to say that $\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right] = 1$. These numbers thus form a triangle in the obvious way, just as the Stirling numbers of the first kind do. Here are lines 1–5 of the triangle:

$$\begin{array}{cccccc} 1 & & & & & \\ 0 & 1 & & & & \\ 0 & 1 & 1 & & & \\ 0 & 2 & 3 & 1 & & \\ 0 & 6 & 11 & 6 & 1 & \\ 0 & 24 & 50 & 35 & 10 & 1 \end{array}$$

The first column is not particularly interesting, so often it is eliminated.

In exercise 4 in section 1.4, we saw that

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}. \tag{1.8.1}$$

The unsigned Stirling numbers of the first kind satisfy a similar recurrence.

THEOREM 1.8.3 $\left[\begin{smallmatrix}n\\k\end{smallmatrix}\right] = \left[\begin{smallmatrix}n-1\\k-1\end{smallmatrix}\right] + (n-1) \cdot \left[\begin{smallmatrix}n-1\\k\end{smallmatrix}\right]$, $k \geq 1$, $n \geq 1$.

Proof. The proof is by induction on n; the table above shows that it is true for the first few lines. We split the permutations of $[n]$ with k cycles into two types: those in which (n) is a 1-cycle, and the rest. If (n) is a 1-cycle, then the remaining cycles form a permutation of $[n-1]$ with $k-1$ cycles, so there are $\left[\begin{smallmatrix}n-1\\k-1\end{smallmatrix}\right]$ of these. Otherwise, n occurs in a cycle of length at least 2, and removing n leaves a permutation of $[n-1]$ with k cycles. Given a permutation σ of $[n-1]$ with k cycles, n can be added to any cycle in any position to form a permutation of $[n]$ in which (n) is not a 1-cycle. Suppose the lengths of the cycles in σ are $l_1, l_2, \ldots, l_k$. In cycle number i, n may be added after any of the l_i elements in the cycle. Thus, the total number of places that n can be added is $l_1 + l_2 + \cdots + l_k = n-1$, so there are $(n-1) \cdot \left[\begin{smallmatrix}n-1\\k\end{smallmatrix}\right]$ permutations of $[n]$ in which (n) is not a 1-cycle. Now the total number of permutations of $[n]$ with k cycles is $\left[\begin{smallmatrix}n-1\\k-1\end{smallmatrix}\right] + (n-1) \cdot \left[\begin{smallmatrix}n-1\\k\end{smallmatrix}\right]$, as desired. ■

COROLLARY 1.8.4 $s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k)$. ■

The Stirling numbers satisfy two remarkable identities. First a definition:

DEFINITION 1.8.5 The **Kronecker delta** $\delta_{n,k}$ is 1 if $n = k$ and 0 otherwise. □

THEOREM 1.8.6 For $n \geq 0$ and $k \geq 0$,

$$\sum_{j=0}^{n} s(n,j)S(j,k) = \sum_{j=0}^{n} (-1)^{n-j} \left[{n \atop j} \right] \left\{ {j \atop k} \right\} = \delta_{n,k}$$

$$\sum_{j=0}^{n} S(n,j)s(j,k) = \sum_{j=0}^{n} (-1)^{j-k} \left\{ {n \atop j} \right\} \left[{j \atop k} \right] = \delta_{n,k}$$

Proof. We prove the first version, by induction on n. The first few values of n are easily checked; assume $n > 1$. Now note that $\left[\begin{smallmatrix} n \\ 0 \end{smallmatrix}\right] = 0$, so we may start the sum index j at 1.

When $k > n$, $\left\{\begin{smallmatrix} j \\ k \end{smallmatrix}\right\} = 0$, for $1 \le j \le n$, and so the sum is 0. When $k = n$, the only non-zero term occurs when $j = n$, and is $(-1)^0 \left[\begin{smallmatrix} n \\ n \end{smallmatrix}\right] \left\{\begin{smallmatrix} n \\ n \end{smallmatrix}\right\} = 1$, so the sum is 1. Now suppose $k < n$. When $k = 0$, $\left\{\begin{smallmatrix} j \\ k \end{smallmatrix}\right\} = 0$ for $j > 0$, so the sum is 0, and we assume now that $k > 0$.

We begin by applying the recurrence relations:

$$\begin{aligned}
\sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} &= \sum_{j=1}^{n}(-1)^{n-j} \left(\begin{bmatrix} n-1 \\ j-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} \right) \begin{Bmatrix} j \\ k \end{Bmatrix} \\
&= \sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} + \sum_{j=1}^{n}(-1)^{n-j}(n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} \\
&= \sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \left(\begin{Bmatrix} j-1 \\ k-1 \end{Bmatrix} + k \begin{Bmatrix} j-1 \\ k \end{Bmatrix} \right) + \sum_{j=1}^{n}(-1)^{n-j}(n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} \\
&= \sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \begin{Bmatrix} j-1 \\ k-1 \end{Bmatrix} + \sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} k \begin{Bmatrix} j-1 \\ k \end{Bmatrix} \\
&\quad + \sum_{j=1}^{n}(-1)^{n-j}(n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix}.
\end{aligned}$$

Consider the first sum in the last expression:

$$\begin{aligned}
\sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \begin{Bmatrix} j-1 \\ k-1 \end{Bmatrix} &= \sum_{j=2}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \begin{Bmatrix} j-1 \\ k-1 \end{Bmatrix} \\
&= \sum_{j=1}^{n-1}(-1)^{n-j-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k-1 \end{Bmatrix} \\
&= \delta_{n-1,k-1} = 0,
\end{aligned}$$

since $k - 1 < n - 1$ (or trivially, if $k = 1$). Thus, we are left with just two sums.

$$\begin{aligned}
&\sum_{j=1}^{n}(-1)^{n-j} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} k \begin{Bmatrix} j-1 \\ k \end{Bmatrix} + \sum_{j=1}^{n}(-1)^{n-j}(n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} \\
&\quad = k \sum_{j=1}^{n-1}(-1)^{n-j-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} - (n-1) \sum_{j=1}^{n-1}(-1)^{n-j-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \begin{Bmatrix} j \\ k \end{Bmatrix} \\
&\quad = k\delta_{n-1,k} - (n-1)\delta_{n-1,k}.
\end{aligned}$$

Now if $k = n - 1$, this is $(n-1)\delta_{n-1,n-1} - (n-1)\delta_{n-1,n-1} = 0$, while if $k < n - 1$ it is $k\delta_{n-1,k} - (n-1)\delta_{n-1,k} = k \cdot 0 - (n-1) \cdot 0 = 0$. ∎

If we interpret the triangles containing the $s(n,k)$ and $S(n,k)$ as matrices, either $m \times m$, by taking the first m rows and columns, or even the infinite matrices containing the entire triangles, the sums of the theorem correspond to computing the matrix product in both orders. The theorem then says that this product consists of ones on the diagonal and zeros elsewhere, so these matrices are inverses. Here is a small example:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 & 0 \\ 0 & -6 & 11 & -6 & 1 & 0 \\ 0 & 24 & -50 & 35 & -10 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 7 & 6 & 1 & 0 \\ 0 & 1 & 15 & 25 & 10 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Exercises 1.8.

1. Find a simple expression for $\begin{bmatrix} n \\ n-1 \end{bmatrix}$.

2. Find a simple expression for $\begin{bmatrix} n \\ 1 \end{bmatrix}$.

3. What is $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}$?

4. What is $\sum_{k=0}^{n} s(n,k)$?

5. Show that $x^{\underline{n}} = \prod_{k=0}^{n-1}(x-k) = \sum_{i=0}^{n} s(n,i)x^i$, $n \geq 1$; $x^{\underline{n}}$ is called a **falling factorial**. Find a similar identity for $x^{\overline{n}} = \prod_{k=0}^{n-1}(x+k)$; $x^{\overline{n}}$ is a **rising factorial**.

6. Show that $\displaystyle\sum_{k=0}^{n} \left\{ n \atop k \right\} x^{\underline{k}} = x^n$, $n \geq 1$; $x^{\underline{k}}$ is defined in the previous exercise. The previous exercise shows how to express the falling factorial in terms of powers of x; this exercise shows how to express the powers of x in terms of falling factorials.

7. Prove: $\displaystyle S(n,k) = \sum_{i=k-1}^{n-1} \binom{n-1}{i} S(i,k-1)$.

8. Prove: $\displaystyle \begin{bmatrix} n \\ k \end{bmatrix} = \sum_{i=k-1}^{n-1} (n-i-1)! \binom{n-1}{i} \begin{bmatrix} i \\ k-1 \end{bmatrix}$.

9. Use the previous exercise to prove $\displaystyle s(n,k) = \sum_{i=k-1}^{n-1} (-1)^{n-i-1}(n-i-1)! \binom{n-1}{i} s(i,k-1)$.

10. We have defined $\begin{bmatrix} n \\ k \end{bmatrix}$ and $\left\{ n \atop k \right\}$ for $n, k \geq 0$. We want to extend the definitions to all integers. Without some extra stipulations, there are many ways to do this. Let us suppose that for $n \neq 0$ we want $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ n \end{bmatrix} = \left\{ n \atop 0 \right\} = \left\{ 0 \atop n \right\} = 0$, and we want the recurrence relations of equation 1.8.1 and in theorem 1.8.3 to be true. Show that under these conditions there is a unique way to extend the definitions to all integers, and that when this is done, $\left\{ n \atop k \right\} = \begin{bmatrix} -k \\ -n \end{bmatrix}$ for all integers n and k. Thus, the extended table of values for either $\begin{bmatrix} n \\ k \end{bmatrix}$ or $\left\{ n \atop k \right\}$ will contain all the values of both $\begin{bmatrix} n \\ k \end{bmatrix}$ and $\left\{ n \atop k \right\}$.

11. Under the assumptions that $s(n,0) = s(0,n) = 0$ for $n \neq 0$, and $s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k)$, extend the table for $s(n,k)$ to all integers, and find a connection to $S(n,k)$ similar to that in the previous problem.

12. Prove corollary 1.8.4.

13. Prove the remaining part of theorem 1.8.6.

2

Inclusion-Exclusion

2.1 The Inclusion-Exclusion Formula

Let's return to a problem we have mentioned but not solved:

EXAMPLE 2.1.1 How many submultisets of the multiset $\{2 \cdot a, 4 \cdot b, 3 \cdot c\}$ have size 7?

We recast the problem: this is the number of solutions to $x_1 + x_2 + x_3 = 7$ with $0 \le x_1 \le 2$, $0 \le x_2 \le 4$, $0 \le x_3 \le 3$. We know that the number of solutions in non-negative integers is $\binom{7+3-1}{3-1} = \binom{9}{2}$, so this is an overcount, since we count solutions that do not meet the upper bound restrictions. For example, this includes some solutions with $x_1 \ge 3$; how many of these are there? This is a problem we can solve: it is the number of solutions to $x_1 + x_2 + x_3 = 7$ with $3 \le x_1$, $0 \le x_2$, $0 \le x_3$. This is the same as the number of non-negative solutions of $y_1 + y_2 + y_3 = 7 - 3 = 4$, or $\binom{4+3-1}{3-1} = \binom{6}{2}$. Thus, $\binom{9}{2} - \binom{6}{2}$ corrects this overcount. If we likewise correct for the overcounting of solutions with $x_2 \ge 5$ and $x_3 \ge 4$, we get $\binom{9}{2} - \binom{6}{2} - \binom{4}{2} - \binom{5}{2}$. Is this correct? Not necessarily, because we now have a potential undercount: we have twice subtracted 1 for a solution in which both $x_1 \ge 3$ and $x_2 \ge 5$, when we should have subtracted just 1. However, by good fortune, there are no such solutions, since $3 + 5 > 7$. But the same applies to the other pairs of variables: How many solutions have $x_1 \ge 3$ and $x_3 \ge 4$? It's easy to see there is only one such solution, namely $3 + 0 + 4 = 7$. Finally, there are no solutions with $x_2 \ge 5$ and $x_3 \ge 4$, so the corrected count is now $\binom{9}{2} - \binom{6}{2} - \binom{4}{2} - \binom{5}{2} + 1$. This does not take into account any solutions in which $x_1 \ge 3$, $x_2 \ge 5$, and $x_3 \ge 4$, but there are none of these, so the actual count is

$$\binom{9}{2} - \binom{6}{2} - \binom{4}{2} - \binom{5}{2} + 1 = 36 - 15 - 6 - 10 + 1 = 6.$$

This is small enough that it is not hard to verify by listing all the solutions. □

So we solved this problem, but it is apparent that it could have been much worse, if the number of variables were larger and there were many complicated overcounts and undercounts. Remarkably, it is possible to streamline this sort of argument; it will still, often, be quite messy, but the reasoning will be simpler.

Let's start by rephrasing the example. Let S be the set of all non-negative solutions to $x_1 + x_2 + x_3 = 7$, let A_1 be all solutions with $x_1 \geq 3$, A_2 all solutions with $x_2 \geq 5$, and A_3 all solutions with $x_3 \geq 4$. We want to know the size of $A_1^c \cap A_2^c \cap A_3^c$, the solutions for which it is not true that $x_1 \geq 3$ and not true that $x_2 \geq 5$ and not true that $x_3 \geq 4$. Examining our solution, we see that the final count is

$$\begin{aligned} &|S| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| \\ &\qquad = 36 - 15 - 6 - 10 + 0 + 1 + 0 - 0. \end{aligned}$$

This pattern is completely general:

THEOREM 2.1.2 The inclusion-exclusion formula If $A_i \subseteq S$ for $1 \leq i \leq n$ then

$$|A_1^c \cap \cdots \cap A_n^c| = |S| - |A_1| - \cdots - |A_n| + |A_1 \cap A_2| + \cdots - |A_1 \cap A_2 \cap A_3| - \cdots,$$

or more compactly:

$$|\bigcap_{i=1}^{n} A_i^c| = |S| + \sum_{k=1}^{n} (-1)^k \sum |\bigcap_{j=1}^{k} A_{i_j}|,$$

where the internal sum is over all subsets $\{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$. Alternately we may write

$$|\bigcap_{i=1}^{n} A_i^c| = \sum_{I \subseteq [n]} (-1)^{|I|} |\bigcap_{j \in I} A_j|.$$

(Note that $\bigcap_{j \in \emptyset} A_j = S$.)

Proof. We need to show that each element of $\bigcap_{i=1}^{n} A_i^c$ is counted once by the right hand side, and every other element of S is counted zero times. The first of these is easy: if $x \in \bigcap_{i=1}^{n} A_i^c$ then for every i, $x \notin A_i$, so x is in none of the sets involving the A_i on the right hand side, and so x is counted, once, by the term $|S|$.

Now suppose $x \notin \bigcap_{i=1}^{n} A_i^c$. On the right hand side, x is counted once by the term $|S|$. For some values $i_1, i_2, \ldots, i_k$, $x \in A_{i_m}$, $1 \leq m \leq k$, and x is not in the remaining sets A_i. Then x is counted zero times by any term involving an A_i with $i \notin \{i_1, i_2, \ldots, i_k\}$, and is counted once, positively or negatively, by each term involving only $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$. There are k terms of the form $-|A_{i_m}|$, which count x a total of $-k$ times. There are $\binom{k}{2}$

terms of the form $|A_{i_l} \cap A_{i_m}|$, counting x a total of $\binom{k}{2}$ times. Continuing in this way, we see that the final count for x on the right hand side is

$$1 - k + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \binom{k}{k},$$

or more compactly

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

We know that this alternating sum of binomial coefficients is zero, so x is counted zero times, as desired. (See equation 1.3.1.) ■

An alternate form of the inclusion exclusion formula is sometimes useful.

COROLLARY 2.1.3 If $A_i \subseteq S$ for $1 \leq i \leq n$ then

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum |\bigcap_{j=1}^{k} A_{i_j}|,$$

where the internal sum is over all subsets $\{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$.

Proof. Since $(\bigcup_{i=1}^{n} A_i)^c = \bigcap_{i=1}^{n} A_i^c$,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= |S| - |\bigcap_{i=1}^{n} A_i^c| \\
&= |S| - (|S| + \sum_{k=1}^{n} (-1)^k \sum |\bigcap_{j=1}^{k} A_{i_j}|) \\
&= (-1) \sum_{k=1}^{n} (-1)^k \sum |\bigcap_{j=1}^{k} A_{i_j}| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum |\bigcap_{j=1}^{k} A_{i_j}|.
\end{aligned}$$

■

Since the right hand side of the inclusion-exclusion formula consists of 2^n terms to be added, it can still be quite tedious. In some nice cases, all intersections of the same number of sets have the same size. Since there are $\binom{n}{k}$ possible intersections consisting of k sets, the formula becomes

$$|\bigcap_{i=1}^{n} A_i^c| = |S| + \sum_{k=1}^{n} (-1)^k \binom{n}{k} m_k, \tag{2.1.1}$$

where m_k is the size of an intersection of k of the sets.

EXAMPLE 2.1.4 Find the number of solutions to $x_1+x_2+x_3+x_4 = 25$, $0 \le x_i \le 10$. Let A_i be the solutions of $x_1 + x_2 + x_3 + x_4 = 25$ with $x_i \ge 11$. The number of solutions with $x_i \ge 0$ for all i is $\binom{25+4-1}{4-1} = \binom{25+3}{3}$. Also $|A_i| = \binom{14+3}{3}$, and $|A_i \cap A_j| = \binom{3+3}{3}$. There are no solutions with 3 or 4 of the variables larger than 10. Hence the number of solutions is

$$\binom{25+3}{3} - \binom{4}{1}\binom{14+3}{3} + \binom{4}{2}\binom{3+3}{3} = 676.$$

□

Exercises 2.1.

1. List all 6 solutions to the restricted equation in example 2.1.1, and list the corresponding 6 submultisets.
2. Find the number of integer solutions to $x_1 + x_2 + x_3 + x_4 = 25$, $1 \le x_1 \le 6$, $2 \le x_2 \le 8$, $0 \le x_3 \le 8$, $5 \le x_4 \le 9$.
3. Find the number of submultisets of $\{25 \cdot a, 25 \cdot b, 25 \cdot c, 25 \cdot d\}$ of size 80.
4. Recall that $\left\{ {n \atop k} \right\}$ is a Stirling number of the second kind (definition 1.8.1). Prove that for $n \ge k \ge 0$,

$$\left\{ {n \atop k} \right\} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}i^n\binom{k}{i}.$$

   Do $n = 0$ as a special case, then use inclusion-exclusion for the rest. You may assume, by convention, that $0^0 = 1$.

2.2 Forbidden Position Permutations

Suppose we shuffle a deck of cards; what is the probability that no card is in its original location? More generally, how many permutations of $[n] = \{1, 2, 3, \ldots, n\}$ have none of the integers in their "correct" locations? That is, 1 is not first, 2 is not second, and so on. Such a permutation is called a **derangement** of $[n]$.

Let S be the set of all permutations of $[n]$ and A_i be the permutations of $[n]$ in which i is in the correct place. Then we want to know $|\bigcap_{i=1}^{n} A_i^c|$.

For any i, $|A_i| = (n-1)!$: once i is fixed in position i, the remaining $n-1$ integers can be placed in any locations.

What about $|A_i \cap A_j|$? If both i and j are in the correct position, the remaining $n-2$ integers can be placed anywhere, so $|A_i \cap A_j| = (n-2)!$.

In the same way, we see that $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = (n-k)!$. Thus, by the inclusion-exclusion formula, in the form of equation 2.1.1,

$$\begin{aligned}
|\bigcap_{i=1}^{n} A_i^c| &= |S| + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! \\
&= n! + \sum_{k=1}^{n} (-1)^k \frac{n!}{k!(n-k)!} (n-k)! \\
&= n! + \sum_{k=1}^{n} (-1)^k \frac{n!}{k!} \\
&= n! + n! \sum_{k=1}^{n} (-1)^k \frac{1}{k!} \\
&= n! \left(1 + \sum_{k=1}^{n} (-1)^k \frac{1}{k!}\right) \\
&= n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}.
\end{aligned}$$

The last sum should look familiar:

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Substituting $x = -1$ gives

$$e^{-1} = \sum_{k=0}^{\infty} \frac{1}{k!} (-1)^k.$$

The probability of getting a derangement by chance is then

$$\frac{1}{n!} n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!},$$

and when n is bigger than 6, this is quite close to

$$e^{-1} \approx 0.3679.$$

So in the case of a deck of cards, the probability of a derangement is about 37%.

Let $D_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$. These **derangement numbers** have some interesting properties. First, note that when $n = 0$, we have $D_0 = 0!(-1)^0 \frac{1}{0!} = 1$. "Derangements of the empty set" doesn't really make sense, but it is useful to adopt the convention that $D_0 = 1$.

The derangements of $[n]$ may be produced as follows: For each $i \in \{2, 3, \ldots, n\}$, put i in position 1 and 1 in position i. Then permute the numbers $\{2, 3, \ldots, i-1, i+1, \ldots n\}$ in all possible ways so that none of these $n-2$ numbers is in the correct place. There are D_{n-2} ways to do this. Then, keeping 1 in position i, derange the numbers $\{i, 2, 3, \ldots, i-1, i+1, \ldots n\}$, with the "correct" position of i now considered to be position 1. There are D_{n-1} ways to do this. Thus, $D_n = (n-1)(D_{n-1} + D_{n-2})$. Starting with $D_0 = 1$ and $D_1 = 0$, this gives $D_2 = (1)(0+1) = 1$ and $D_3 = (2)(1+0) = 2$, both of which are easy to check directly.

We explore this **recurrence relation** a bit:

$$\begin{aligned}
D_n &= nD_{n-1} - D_{n-1} + (n-1)D_{n-2} && (*)\\
&= nD_{n-1} - (n-2)(D_{n-2} + D_{n-3}) + (n-1)D_{n-2}\\
&= nD_{n-1} - (n-2)D_{n-2} - (n-2)D_{n-3} + (n-1)D_{n-2}\\
&= nD_{n-1} + D_{n-2} - (n-2)D_{n-3} && (*)\\
&= nD_{n-1} + (n-3)(D_{n-3} + D_{n-4}) - (n-2)D_{n-3}\\
&= nD_{n-1} + (n-3)D_{n-3} + (n-3)D_{n-4} - (n-2)D_{n-3}\\
&= nD_{n-1} - D_{n-3} + (n-3)D_{n-4} && (*)\\
&= nD_{n-1} - (n-4)(D_{n-4} + D_{n-5}) + (n-3)D_{n-4}\\
&= nD_{n-1} - (n-4)D_{n-4} - (n-4)D_{n-5} + (n-3)D_{n-4}\\
&= nD_{n-1} + D_{n-4} - (n-4)D_{n-5}. && (*)
\end{aligned}$$

It appears from the starred lines that the pattern here is that

$$D_n = nD_{n-1} + (-1)^k D_{n-k} + (-1)^{k+1}(n-k)D_{n-k-1}.$$

If this continues, we should get to

$$D_n = nD_{n-1} + (-1)^{n-2}D_2 + (-1)^{n-1}(2)D_1.$$

Since $D_2 = 1$ and $D_1 = 0$, this would give

$$D_n = nD_{n-1} + (-1)^n,$$

since $(-1)^n = (-1)^{n-2}$. Indeed this is true, and can be proved by induction. This gives a somewhat simpler recurrence relation, making it quite easy to compute D_n.

• • •

There are many similar problems.

EXAMPLE 2.2.1 How many permutations of $[n]$ contain no instance of i followed by $i+1$?

By a similar use of the inclusion-exclusion formula, it turns out that this is

$$Q_n = n! \sum_{k=0}^{n-1} (-1)^k \frac{1}{k!} + (n-1)! \sum_{k=1}^{n-1} (-1)^{k-1} \frac{1}{(k-1)!}.$$

Note that the limits on the two sums are not identical. □

Exercises 2.2.

1. Prove that $D_n = nD_{n-1} + (-1)^n$ when $n \geq 1$, by induction on n.

2. Prove that D_n is even if and only if n is odd.

3. Provide the missing details for example 2.2.1. What is $\lim_{n\to\infty} \frac{Q_n}{n!}$?

4. Find the number of permutations of $1, 2, \ldots, 8$ that have no odd number in the correct position.

5. Find the number of permutations of $1, 2, \ldots, 8$ that have at least one odd number in the correct position.

6. How many permutations of $[n]$ have exactly k numbers in their correct positions?

7. Give a combinatorial proof that

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}.$$

8. A small merry-go-round has 8 seats occupied by 8 children. In how many ways can the children change places so that no child sits behind the same child as on the first ride? The seats do not matter, only the relative positions of the children.

9. Repeat the previous problem with n instead of 8.

10. On the way into a party everyone checks a coat and a bag at the door. On the way out, the attendant hands out coats and bags randomly. In how many ways can this be done if

(a) No one gets either their own coat or their own bag?

(b) One may get one's own coat, or bag, but not both.

11. Suppose n people are seated in $m \geq n$ chairs in a room. At some point there is a break, and everyone leaves the room. When they return, in how many ways can they be seated so that no person occupies the same chair as before the break?

3

Generating Functions

As we have seen, a typical counting problem includes one or more parameters, which of course show up in the solutions, such as $\binom{n}{k}$, $P(n,k)$, or the number of derangements of $[n]$. Also recall that

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

This provides the values $\binom{n}{k}$ as coefficients of the Maclaurin expansion of a function. This turns out to be a useful idea.

DEFINITION 3.0.1 $f(x)$ is a **generating function** for the sequence $a_0, a_1, a_2, \ldots$ if

$$f(x) = \sum_{i=0}^{\infty} a_i x^i.$$

□

Sometimes a generating function can be used to find a formula for its coefficients, but if not, it gives a way to generate them. Generating functions can also be useful in proving facts about the coefficients.

3.1 Newton's Binomial Theorem

Recall that

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

The expression on the right makes sense even if n is not a non-negative integer, so long as k is a non-negative integer, and we therefore define

$$\binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-k+1)}{k!}$$

when r is a real number. For example,

$$\binom{1/2}{4} = \frac{(1/2)(-1/2)(-3/2)(-5/2)}{4!} = \frac{-5}{128} \quad \text{and} \quad \binom{-2}{3} = \frac{(-2)(-3)(-4)}{3!} = -4.$$

These **generalized binomial coefficients** share some important properties of the usual binomial coefficients, most notably that

$$\binom{r}{k} = \binom{r-1}{k-1} + \binom{r-1}{k}. \tag{3.1.1}$$

Then remarkably:

THEOREM 3.1.1 Newton's Binomial Theorem For any real number r that is not a non-negative integer,

$$(x+1)^r = \sum_{i=0}^{\infty} \binom{r}{i} x^i$$

when $-1 < x < 1$.

Proof. It is not hard to see that the series is the Maclaurin series for $(x+1)^r$, and that the series converges when $-1 < x < 1$. It is rather more difficult to prove that the series is equal to $(x+1)^r$; the proof may be found in many introductory real analysis books. ■

EXAMPLE 3.1.2 Expand the function $(1-x)^{-n}$ when n is a positive integer.

We first consider $(x+1)^{-n}$; we can simplify the binomial coefficients:

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

Thus

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

Now replacing x by $-x$ gives

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

So $(1-x)^{-n}$ is the generating function for $\binom{n+i-1}{n-1}$, the number of submultisets of $\{\infty \cdot 1, \infty \cdot 2, \ldots, \infty \cdot n\}$ of size i. □

In many cases it is possible to directly construct the generating function whose coefficients solve a counting problem.

EXAMPLE 3.1.3 Find the number of solutions to $x_1 + x_2 + x_3 + x_4 = 17$, where $0 \le x_1 \le 2$, $0 \le x_2 \le 5$, $0 \le x_3 \le 5$, $2 \le x_4 \le 6$.

We can of course solve this problem using the inclusion-exclusion formula, but we use generating functions. Consider the function

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

We can multiply this out by choosing one term from each factor in all possible ways. If we then collect like terms, the coefficient of x^k will be the number of ways to choose one term from each factor so that the exponents of the terms add up to k. This is precisely the number of solutions to $x_1 + x_2 + x_3 + x_4 = k$, where $0 \le x_1 \le 2$, $0 \le x_2 \le 5$, $0 \le x_3 \le 5$, $2 \le x_4 \le 6$. Thus, the answer to the problem is the coefficient of x^{17}. With the help of a computer algebra system we get

$$\begin{aligned}(1+x+x^2)(1+x+x^2+x^3+x^4+x^5)^2(x^2+x^3+x^4+x^5+x^6)&\\ = x^{18} + 4x^{17} + 10x^{16} + 19x^{15} + 31x^{14} + 45x^{13} + 58x^{12} + 67x^{11} + 70x^{10}&\\ + 67x^9 + 58x^8 + 45x^7 + 31x^6 + 19x^5 + 10x^4 + 4x^3 + x^2,&\end{aligned}$$

so the answer is 4. □

EXAMPLE 3.1.4 Find the generating function for the number of solutions to $x_1 + x_2 + x_3 + x_4 = k$, where $0 \le x_1 \le \infty$, $0 \le x_2 \le 5$, $0 \le x_3 \le 5$, $2 \le x_4 \le 6$.

This is just like the previous example except that x_1 is not bounded above. The generating function is thus

$$\begin{aligned}f(x) &= (1+x+x^2+\cdots)(1+x+x^2+x^3+x^4+x^5)^2(x^2+x^3+x^4+x^5+x^6)\\ &= (1-x)^{-1}(1+x+x^2+x^3+x^4+x^5)^2(x^2+x^3+x^4+x^5+x^6)\\ &= \frac{(1+x+x^2+x^3+x^4+x^5)^2(x^2+x^3+x^4+x^5+x^6)}{1-x}.\end{aligned}$$

Note that $(1-x)^{-1} = (1+x+x^2+\cdots)$ is the familiar geometric series from calculus; alternately, we could use example 3.1.2. Unlike the function in the previous example, this function has an infinite expansion:

$$\begin{aligned}f(x) = x^2 &+ 4x^3 + 10x^4 + 20x^5 + 35x^6 + 55x^7 + 78x^8\\ &+ 102x^9 + 125x^{10} + 145x^{11} + 160x^{12} + 170x^{13} + 176x^{14}\\ &+ 179x^{15} + 180x^{16} + 180x^{17} + 180x^{18} + 180x^{19} + 180x^{20} + \cdots.\end{aligned}$$

You can see how to do this in Sage. □

EXAMPLE 3.1.5 Find a generating function for the number of submultisets of $\{\infty \cdot a, \infty \cdot b, \infty \cdot c\}$ in which there are an odd number of as, an even number of bs, and any number of cs. As we have seen, this is the same as the number of solutions to $x_1 + x_2 + x_3 = n$ in which x_1 is odd, x_2 is even, and x_3 is unrestricted. The generating function is therefore

$$\begin{aligned}(x + x^3 + x^5 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x + x^2 + x^3 + \cdots) \\ &= x(1 + (x^2) + (x^2)^2 + (x^2)^3 + \cdots)(1 + (x^2) + (x^2)^2 + (x^2)^3 + \cdots)\frac{1}{1-x} \\ &= \frac{x}{(1-x^2)^2(1-x)}.\end{aligned}$$

□

Exercises 3.1.

For some of these exercises, you may want to use the sage applet above, in example 3.1.4, or your favorite computer algebra system.

1. Prove that $\binom{r}{k} = \binom{r-1}{k-1} + \binom{r-1}{k}$.
2. Show that the Maclaurin series for $(x+1)^r$ is $\sum_{i=0}^{\infty} \binom{r}{i} x^i$.
3. Concerning example 3.1.4, show that all coefficients beginning with x^{16} are 180.
4. Use a generating function to find the number of solutions to $x_1 + x_2 + x_3 + x_4 = 14$, where $0 \le x_1 \le 3$, $2 \le x_2 \le 5$, $0 \le x_3 \le 5$, $4 \le x_4 \le 6$.
5. Find the generating function for the number of solutions to $x_1 + x_2 + x_3 + x_4 = k$, where $0 \le x_1 \le \infty$, $3 \le x_2 \le \infty$, $2 \le x_3 \le 5$, $1 \le x_4 \le 5$.
6. Find a generating function for the number of non-negative integer solutions to $3x + 2y + 7z = n$.
7. Suppose we have a large supply of red, white, and blue balloons. How many different bunches of 10 balloons are there, if each bunch must have at least one balloon of each color and the number of white balloons must be even?
8. Use generating functions to show that every positive integer can be written in exactly one way as a sum of distinct powers of 2.
9. Suppose we have a large supply of blue and green candles, and one gold candle. How many collections of n candles are there in which the number of blue candles is even, the number of green candles is any number, and the number of gold candles is at most one?

3.2 Exponential Generating Functions

There are other ways that a function might be said to generate a sequence, other than as what we have called a generating function. For example,

$$e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

is the generating function for the sequence $1, 1, \frac{1}{2}, \frac{1}{3!}, \ldots$. But if we write the sum as

$$e^x = \sum_{n=0}^{\infty} 1 \cdot \frac{x^n}{n!},$$

considering the $n!$ to be part of the expression $x^n/n!$, we might think of this same function as generating the sequence $1, 1, 1, \ldots$, interpreting 1 as the coefficient of $x^n/n!$. This is not a very interesting sequence, of course, but this idea can often prove fruitful. If

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!},$$

we say that $f(x)$ is the **exponential generating function** for $a_0, a_1, a_2, \ldots$.

EXAMPLE 3.2.1 Find an exponential generating function for the number of permutations with repetition of length n of the set $\{a, b, c\}$, in which there are an odd number of as, an even number of bs, and any number of cs.

For a fixed n and fixed numbers of the letters, we already know how to do this. For example, if we have 3 as, 4 bs, and 2 cs, there are $\binom{9}{3\,4\,2}$ such permutations. Now consider the following function:

$$\sum_{i=0}^{\infty} \frac{x^{2i+1}}{(2i+1)!} \sum_{i=0}^{\infty} \frac{x^{2i}}{(2i)!} \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

What is the coefficient of $x^9/9!$ in this product? One way to get an x^9 term is

$$\frac{x^3}{3!}\frac{x^4}{4!}\frac{x^2}{2!} = \frac{9!}{3!\,4!\,2!}\frac{x^9}{9!} = \binom{9}{3\,4\,2}\frac{x^9}{9!}.$$

That is, this one term counts the number of permutations in which there are 3 as, 4 bs, and 2 cs. The ultimate coefficient of $x^9/9!$ will be the sum of many such terms, counting the contributions of all possible choices of an odd number of as, an even number of bs, and any number of cs.

Now we notice that $\displaystyle\sum_{i=0}^{\infty} \frac{x^i}{i!} = e^x$, and that the other two sums are closely related to this. A little thought leads to

$$e^x + e^{-x} = \sum_{i=0}^{\infty} \frac{x^i}{i!} + \sum_{i=0}^{\infty} \frac{(-x)^i}{i!} = \sum_{i=0}^{\infty} \frac{x^i + (-x)^i}{i!}.$$

Now $x^i + (-x)^i$ is $2x^i$ when i is even, and 0 when i is odd. Thus

$$e^x + e^{-x} = \sum_{i=0}^{\infty} \frac{2x^{2i}}{(2i)!},$$

so that

$$\sum_{i=0}^{\infty} \frac{x^{2i}}{(2i)!} = \frac{e^x + e^{-x}}{2}.$$

A similar manipulation shows that

$$\sum_{i=0}^{\infty} \frac{x^{2i+1}}{(2i+1)!} = \frac{e^x - e^{-x}}{2}.$$

Thus, the generating function we seek is

$$\frac{e^x - e^{-x}}{2}\frac{e^x + e^{-x}}{2}e^x = \frac{1}{4}(e^x - e^{-x})(e^x + e^{-x})e^x = \frac{1}{4}(e^{3x} - e^{-x}).$$

Notice the similarity to example 3.1.5. □

Exercises 3.2.

1. Find the coefficient of $x^9/9!$ in the function of example 3.2.1. You may use Sage or a similar program.

2. Find an exponential generating function for the number of permutations with repetition of length n of the set $\{a, b, c\}$, in which there are an odd number of as, an even number of bs, and an even number of cs.

3. Find an exponential generating function for the number of permutations with repetition of length n of the set $\{a, b, c\}$, in which the number of as is even and at least 2, the number of bs is even and at most 6, and the number of cs is at least 3.

4. In how many ways can we paint the 10 rooms of a hotel if at most three can be painted red, at most 2 painted green, at most 1 painted white, and any number can be painted blue or orange? (The rooms are different, so order matters.)

5. Recall from section 1.4 that the Bell numbers B_n count all of the partitions of $\{1, 2, \ldots, n\}$.

Let $f(x) = \sum_{n=0}^{\infty} B_n \cdot \frac{x^n}{n!}$, and note that

$$f'(x) = \sum_{n=1}^{\infty} B_n \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} B_{n+1}\frac{x^n}{n!} = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}B_{n-k}\right)\frac{x^n}{n!},$$

using the recurrence relation 1.4.1 for B_{n+1} from section 1.4. Now it is possible to write this as a product of two infinite series:

$$f'(x) = \left(\sum_{n=0}^{\infty} B_n \cdot \frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty} a_n x^n\right) = f(x)g(x).$$

Find an expression for a_n that makes this true, which will tell you what $g(x)$ is, then solve the differential equation for $f(x)$, the exponential generating function for the Bell numbers.

From section 1.4, the first few Bell numbers are 1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437. You can use Sage to check your answer.

3.3 Partitions of Integers

DEFINITION 3.3.1 A **partition** of a positive integer n is a multiset of positive integers that sum to n. We denote the number of partitions of n by p_n. □

Typically a partition is written as a sum, not explicitly as a multiset. Using the usual convention that an empty sum is 0, we say that $p_0 = 1$.

EXAMPLE 3.3.2 The partitions of 5 are

$$\begin{aligned}
&5\\
&4+1\\
&3+2\\
&3+1+1\\
&2+2+1\\
&2+1+1+1\\
&1+1+1+1+1.
\end{aligned}$$

Thus $p_5 = 7$. □

There is no simple formula for p_n, but it is not hard to find a generating function for them. As with some previous examples, we seek a product of factors so that when the factors are multiplied out, the coefficient of x^n is p_n. We would like each x^n term to represent a single partition, before like terms are collected. A partition is uniquely described by the number of 1s, number of 2s, and so on, that is, by the repetition numbers of the multiset. We devote one factor to each integer:

$$(1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)\cdots(1+x^k+x^{2k}+x^{3k}+\cdots)\cdots = \prod_{k=1}^{\infty}\sum_{i=0}^{\infty} x^{ik}.$$

When this product is expanded, we pick one term from each factor in all possible ways, with the further condition that we only pick a finite number of "non-1" terms. For example, if we pick x^3 from the first factor, x^3 from the third factor, x^{15} from the fifth factor, and 1s from all other factors, we get x^{21}. In the context of the product, this represents $3\cdot 1 + 1\cdot 3 + 3\cdot 5$, corresponding to the partition $1+1+1+3+5+5+5$, that is, three 1s, one 3, and three 5s. Each factor is a geometric series; the kth factor is

$$1 + x^k + (x^k)^2 + (x^k)^3 + \cdots = \frac{1}{1-x^k},$$

so the generating function can be written

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Note that if we are interested in some particular p_n, we do not need the entire infinite product, or even any complete factor, since no partition of n can use any integer greater than n, and also cannot use more than n/k copies of k.

EXAMPLE 3.3.3 Find p_8.

We expand

$$\begin{aligned}(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8)(1+x^2+x^4+x^6+x^8)(1+x^3+x^6)\\ (1+x^4+x^8)(1+x^5)(1+x^6)(1+x^7)(1+x^8)\\ =1+x+2x^2+3x^3+5x^4+7x^5+11x^6+15x^7+22x^8+\cdots+x^{56},\end{aligned}$$

so $p_8 = 22$. Note that all of the coefficients prior to this are also correct, but the following coefficients are not necessarily the corresponding partition numbers. □

Partitions of integers have some interesting properties. Let $p_d(n)$ be the number of partitions of n into distinct parts; let $p_o(n)$ be the number of partitions into odd parts.

EXAMPLE 3.3.4 For $n = 6$, the partitions into distinct parts are

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

so $p_d(6) = 4$, and the partitions into odd parts are

$$5+1, 3+3, 3+1+1+1, 1+1+1+1+1+1,$$

so $p_o(6) = 4$. □

In fact, for every n, $p_d(n) = p_o(n)$, and we can see this by manipulating generating functions. The generating function for $p_d(n)$ is

$$f_d(x) = (1+x)(1+x^2)(1+x^3)\cdots = \prod_{i=1}^{\infty}(1+x^i).$$

The generating function for $p_o(n)$ is

$$f_o(x) = (1+x+x^2+x^3+\cdots)(1+x^3+x^6+x^9+\cdots)\cdots = \prod_{i=0}^{\infty}\frac{1}{1-x^{2i+1}}.$$

We can write

$$f_d(x) = \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdots$$

and notice that every numerator is eventually canceled by a denominator, leaving only the denominators containing odd powers of x, so $f_d(x) = f_o(x)$.

We can also use a recurrence relation to find the partition numbers, though in a somewhat less direct way than the binomial coefficients or the Bell numbers. Let $p_k(n)$ be the number of partitions of n into exactly k parts. We will find a recurrence relation to compute the $p_k(n)$, and then

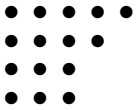
$$p_n = \sum_{k=1}^{n} p_k(n).$$

Now consider the partitions of n into k parts. Some of these partitions contain no 1s, like $3+3+4+6$, a partition of 16 into 4 parts. Subtracting 1 from each part, we get a partition of $n-k$ into k parts; for the example, this is $2+2+3+5$. The remaining partitions of n into k parts contain a 1. If we remove the 1, we are left with a partition of $n-1$ into $k-1$ parts. This gives us a 1–1 correspondence between the partitions of n into k parts, and the partitions of $n-k$ into k parts together with the partitions of $n-1$ into $k-1$ parts, so $p_k(n) = p_k(n-k) + p_{k-1}(n-1)$.

Using this recurrence we can build a triangle containing the $p_k(n)$, and the row sums of this triangle give the partition numbers. For all n, $p_1(n) = 1$, which gives the first column of the triangle, after which the recurrence applies. Also, note that $p_k(n) = 0$ when $k > n$ and we let $p_k(0) = 0$; these are needed in some cases to compute the $p_k(n-k)$ term of the recurrence. Here are the first few rows of the triangle; at the left are the row numbers, and at the right are the row sums, that is, the partition numbers. For the last row, each entry is the sum of the like-colored numbers in the previous rows. Note that beginning with $p_4(7) = 3$ in the last row, $p_k(7) = p_{k-1}(6)$, as $p_k(7-k) = 0$.

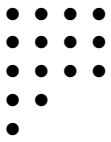
1	1					0		1
2	1	1			0			2
3	1	1	1	0				3
4	1	2	1	1				5
5	1	2	2	1	1			7
6	1	3	3	2	1	1		11
7	1	3	4	3	2	1	1	15

Yet another sometimes useful way to think of a partition is with a **Ferrers diagram**. Each integer in the partition is represented by a row of dots, and the rows are ordered from longest on the top to shortest at the bottom. For example, the partition $3+3+4+5$ would be represented by



The **conjugate** of a partition is the one corresponding to the Ferrers diagram produced by flipping the diagram for the original partition across the main diagonal, thus turning

rows into columns and vice versa. For the diagram above, the conjugate is



with corresponding partition $1 + 2 + 4 + 4 + 4$. This concept can occasionally make facts about partitions easier to see than otherwise. Here is a classic example: the number of partitions of n with largest part k is the same as the number of partitions into k parts, $p_k(n)$. The action of conjugation takes every partition of one type into a partition of the other: the conjugate of a partition into k parts is a partition with largest part k and vice versa. This establishes a 1–1 correspondence between partitions into k parts and partitions with largest part k.

Exercises 3.3.

1. Use generating functions to find p_{15}.
2. Find the generating function for the number of partitions of an integer into distinct odd parts. Find the number of such partitions of 20.
3. Find the generating function for the number of partitions of an integer into distinct even parts. Find the number of such partitions of 30.
4. Find the number of partitions of 25 into odd parts.
5. Find the generating function for the number of partitions of an integer into k parts; that is, the coefficient of x^n is the number of partitions of n into k parts.
6. Complete row 8 of the table for the $p_k(n)$, and verify that the row sum is 22, as we saw in example 3.3.3.
7. A partition of n is self-conjugate if its Ferrers diagram is symmetric around the main diagonal, so that its conjugate is itself. Show that the number of self-conjugate partitions of n is equal to the number of partitions of n into distinct odd parts.

3.4 Recurrence Relations

A **recurrence relation** defines a sequence $\{a_i\}_{i=0}^{\infty}$ by expressing a typical term a_n in terms of earlier terms, a_i for $i < n$. For example, the famous Fibonacci sequence is defined by

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}.$$

Note that some initial values must be specified for the recurrence relation to define a unique sequence.

The starting index for the sequence need not be zero if it doesn't make sense or some other starting index is more convenient. We saw two recurrence relations for the number

of derangements of $[n]$:

$$D_1 = 0, D_n = nD_{n-1} + (-1)^n.$$

and

$$D_1 = 0, D_2 = 1, D_n = (n-1)(D_{n-1} + D_{n-2}).$$

To "solve" a recurrence relation means to find a formula for a_n. There are a variety of methods for solving recurrence relations, with various advantages and disadvantages in particular cases. One method that works for some recurrence relations involves generating functions. The idea is simple, if the execution is not always: Let

$$f(x) = \sum_{i=0}^{\infty} a_i x^i,$$

that is, let $f(x)$ be the generating function for $\{a_i\}_{i=0}^{\infty}$. We now try to manipulate $f(x)$, using the recurrence relation, until we can solve for $f(x)$ explicitly. Finally, we hope that we can find a formula for the coefficients from the formula for $f(x)$.

EXAMPLE 3.4.1 Solve $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$.

Let

$$f(x) = \sum_{i=0}^{\infty} F_i x^i$$

and note that

$$xf(x) = \sum_{i=0}^{\infty} F_i x^{i+1} = \sum_{i=1}^{\infty} F_{i-1} x^i.$$

To get the second sum we have simply "re-indexed" so that the index value gives the exponent on x, just as in the series for $f(x)$. Likewise,

$$x^2 f(x) = \sum_{i=0}^{\infty} F_i x^{i+2} = \sum_{i=2}^{\infty} F_{i-2} x^i.$$

In somewhat more suggestive form, we have

$$\begin{aligned} f(x) &= x + F_2x^2 + F_3x^3 + F_4x^4 + \cdots \\ xf(x) &= \quad x^2 + F_2x^3 + F_3x^4 + \cdots \\ x^2f(x) &= \quad\quad x^3 + F_2x^4 + \cdots \end{aligned}$$

and combining the three equations we get

$$f(x) - xf(x) - x^2f(x) = x + (F_2 - 1)x^2 + (F_3 - F_2 - 1)x^3 + (F_4 - F_3 - F_2)x^4 + \cdots$$

or in more compact form

$$\begin{aligned} f(x) - xf(x) - x^2 f(x) &= \sum_{i=0}^{\infty} F_i x^i - \sum_{i=1}^{\infty} F_{i-1} x^i - \sum_{i=2}^{\infty} F_{i-2} x^i \\ &= x + \sum_{i=2}^{\infty} (F_i - F_{i-1} - F_{i-2}) x^i \\ &= x + \sum_{i=2}^{\infty} 0 \cdot x^i \\ &= x, \end{aligned}$$

recalling that $F_0 = 0$ and $F_1 = 1$. Now

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

If we can find an explicit representation for the series for this function, we will have solved the recurrence relation. Here is where things could go wrong, but in this case it works out. Let a and b be the roots of $x^2 + x - 1$; using the quadratic formula, we get

$$a = \frac{-1 + \sqrt{5}}{2}, b = \frac{-1 - \sqrt{5}}{2}.$$

Borrowing a technique from calculus, we write

$$\frac{-x}{x^2 + x - 1} = \frac{A}{x - a} + \frac{B}{x - b}.$$

Solving for A and B gives

$$A = \frac{1 - \sqrt{5}}{2\sqrt{5}}, B = \frac{-1 - \sqrt{5}}{2\sqrt{5}}.$$

Then

$$\frac{-x}{x^2 + x - 1} = -\frac{A}{a} \frac{1}{1 - x/a} - \frac{B}{b} \frac{1}{1 - x/b}.$$

From calculus we know that

$$\frac{1}{1 - x/a} = \sum_{i=0}^{\infty} (1/a)^i x^i \quad \text{and} \quad \frac{1}{1 - x/b} = \sum_{i=0}^{\infty} (1/b)^i x^i.$$

Finally, this means the coefficient of x^i in the series for $f(x)$ is

$$F_i = -\frac{A}{a}(1/a)^i - \frac{B}{b}(1/b)^i.$$

Simplifying gives

$$F_i = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^i - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^i.$$

Here's an interesting feature of this expression: since $|(1-\sqrt{5})/2| < 1$, the limit of $((1-\sqrt{5})/2)^i$ as i goes to infinity is 0. So when i is large enough,

$$F_i = \text{round}\left(\frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^i\right),$$

that is, the first term rounded to the nearest integer. As it turns out, this is true starting with $i = 0$.

You can see how to do the entire solution in Sage. □

We can also use this expression for F_n to compute $\lim_{n\to\infty} F_n/F_{n-1}$.

$$\lim_{n\to\infty}\frac{F_n}{F_{n-1}} = \lim_{n\to\infty}\frac{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n}{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}} = \frac{1+\sqrt{5}}{2}.$$

This is the so-called "golden ratio".

Exercises 3.4.

1. Find the generating function for the solutions to $h_n = 4h_{n-1} - 3h_{n-2}$, $h_0 = 2$, $h_1 = 5$, and use it to find a formula for h_n.

2. Find the generating function for the solutions to $h_n = 3h_{n-1} + 4h_{n-2}$, $h_0 = h_1 = 1$, and use it to find a formula for h_n.

3. Find the generating function for the solutions to $h_n = 2h_{n-1} + 3^n$, $h_0 = 0$, and use it to find a formula for h_n.

4. Find the generating function for the solutions to $h_n = 4h_{n-2}$, $h_0 = 0$, $h_1 = 1$, and use it to find a formula for h_n. (It is easy to discover this formula directly; the point here is to see that the generating function approach gives the correct answer.)

5. Find the generating function for the solutions to $h_n = h_{n-1} + h_{n-2}$, $h_0 = 1$, $h_1 = 3$, and use it to find a formula for h_n.

6. Find the generating function for the solutions to $h_n = 9h_{n-1} - 26h_{n-2} + 24h_{n-3}$, $h_0 = 0$, $h_1 = 1$, $h_2 = -1$, and use it to find a formula for h_n.

7. Find the generating function for the solutions to $h_n = 3h_{n-1} + 4h_{n-2}$, $h_0 = 0$, $h_1 = 1$, and use it to find a formula for h_n.

8. Find a recursion for the number of ways to place flags on an n foot pole, where we have red flags that are 2 feet high, blue flags that are 1 foot high, and yellow flags that are 1 foot high; the heights of the flags must add up to n. Solve the recursion.

9. In Fibonacci's original problem, a farmer started with one (newborn) pair of rabbits at month 0. After each pair of rabbits was one month old, they produced another pair each month in perpetuity. Thus, after 1 month, he had the original pair, after two months 2 pairs,

three months, 3 pairs, four months, 5 pairs, etc. The number of pairs of rabbits satisfies $h_n = h_{n-1} + h_{n-2}$, $h_0 = h_1 = 1$. (Note that this is slightly different than our definition, in which $h_0 = 0$.)

Suppose instead that each mature pair gives birth to *two* pairs of rabbits. The sequence for the number of pairs of rabbits now starts out $h_0 = 1$, $h_1 = 1$, $h_2 = 3$, $h_3 = 5$, $h_4 = 11$. Set up and solve a recurrence relation for the number of pairs of rabbits. Show also that the sequence statisfies $h_n = 2h_{n-1} + (-1)^n$.

10. Explain why

$$\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n}{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}} = \frac{1+\sqrt{5}}{2}.$$

3.5 Catalan Numbers

A **rooted binary tree** is a type of graph that is particularly of interest in some areas of computer science. A typical rooted binary tree is shown in figure 3.5.1. The root is the topmost vertex. The vertices below a vertex and connected to it by an edge are the children of the vertex. It is a binary tree because all vertices have 0, 1, or 2 children. How many different rooted binary trees are there with n vertices?

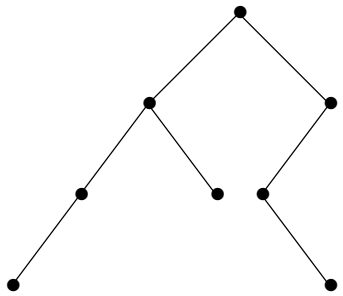


Figure 3.5.1 A rooted binary tree.

Let us denote this number by C_n; these are the **Catalan numbers**. For convenience, we allow a rooted binary tree to be empty, and let $C_0 = 1$. Then it is easy to see that $C_1 = 1$ and $C_2 = 2$, and not hard to see that $C_3 = 5$. Notice that any rooted binary tree on at least one vertex can be viewed as two (possibly empty) binary trees joined into a new tree by introducing a new root vertex and making the children of this root the two roots of the original trees; see figure 3.5.2. (To make the empty tree a child of the new vertex, simply do nothing, that is, omit the corresponding child.)

Thus, to make all possible binary trees with n vertices, we start with a root vertex, and then for its two children insert rooted binary trees on k and l vertices, with $k + l = n - 1$,

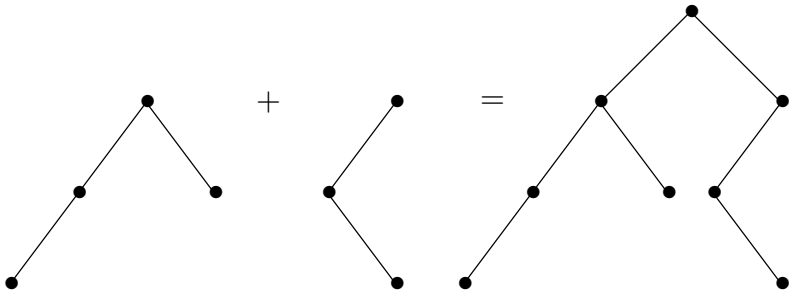


Figure 3.5.2 Producing a new tree from smaller trees.

for all possible choices of the smaller trees. Now we can write

$$C_n = \sum_{i=0}^{n-1} C_i C_{n-i-1}.$$

For example, since we know that $C_0 = C_1 = 1$ and $C_2 = 2$,

$$C_3 = C_0C_2 + C_1C_1 + C_2C_0 = 1 \cdot 2 + 1 \cdot 1 + 2 \cdot 1 = 5,$$

as mentioned above. Once we know the trees on 0, 1, and 2 vertices, we can combine them in all possible ways to list the trees on 3 vertices, as shown in figure 3.5.3. Note that the first two trees have no left child, since the only tree on 0 vertices is empty, and likewise the last two have no right child.

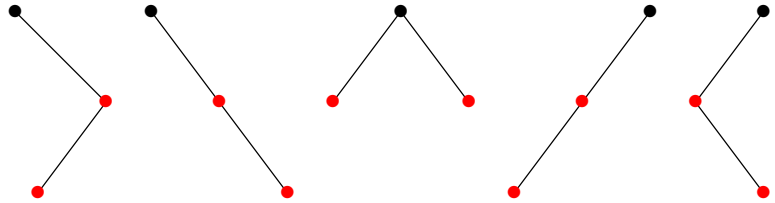


Figure 3.5.3 The 3-vertex binary rooted trees.

Now we use a generating function to find a formula for C_n. Let $f = \sum_{i=0}^{\infty} C_i x^i$. Now consider f^2: the coefficient of the term x^n in the expansion of f^2 is $\sum_{i=0}^{n} C_i C_{n-i}$, corresponding to all possible ways to multiply terms of f to get an x^n term:

$$C_0 \cdot C_n x^n + C_1 x \cdot C_{n-1} x^{n-1} + C_2 x^2 \cdot C_{n-2} x^{n-2} + \cdots + C_n x^n \cdot C_0.$$

Now we recognize this as precisely the sum that gives C_{n+1}, so $f^2 = \sum_{n=0}^{\infty} C_{n+1} x^n$. If we multiply this by x and add 1 (which is C_0) we get exactly f again, that is, $xf^2 + 1 = f$ or $xf^2 - f + 1 = 0$; here 0 is the zero function, that is, $xf^2 - f + 1$ is 0 for all x. Using the

quadratic formula,

$$f = \frac{1 \pm \sqrt{1-4x}}{2x},$$

as long as $x \neq 0$. It is not hard to see that as x approaches 0,

$$\frac{1+\sqrt{1-4x}}{2x}$$

goes to infinity while

$$\frac{1-\sqrt{1-4x}}{2x}$$

goes to 1. Since we know $f(0) = C_0 = 1$, this is the f we want.

Now by Newton's Binomial Theorem 3.1.1, we can expand

$$\sqrt{1-4x} = (1+(-4x))^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-4x)^n.$$

Then

$$\frac{1-\sqrt{1-4x}}{2x} = \sum_{n=1}^{\infty} -\frac{1}{2}\binom{1/2}{n}(-4)^n x^{n-1} = \sum_{n=0}^{\infty} -\frac{1}{2}\binom{1/2}{n+1}(-4)^{n+1}x^n.$$

Expanding the binomial coefficient $\binom{1/2}{n+1}$ and reorganizing the expression, we discover that

$$C_n = -\frac{1}{2}\binom{1/2}{n+1}(-4)^{n+1} = \frac{1}{n+1}\binom{2n}{n}.$$

In exercise 7 in section 1.2, we saw that the number of properly matched sequences of parentheses of length $2n$ is $\binom{2n}{n} - \binom{2n}{n+1}$, and called this C_n. It is not difficult to see that

$$\binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n},$$

so the formulas are in agreement.

Temporarily let A_n be the number of properly matched sequences of parentheses of length $2n$, so from the exercise we know $A_n = \binom{2n}{n} - \binom{2n}{n+1}$. It is possible to see directly that $A_0 = A_1 = 1$ and that the numbers A_n satisfy the same recurrence relation as do the C_n, which implies that $A_n = C_n$, without manipulating the generating function.

There are many counting problems whose answers turns out to be the Catalan numbers. *Enumerative Combinatorics: Volume 2*, by Richard Stanley, contains a large number of examples.

Exercises 3.5.

1. Show that

$$\binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}.$$

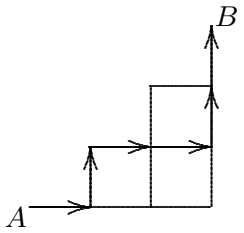
2. Find a simple expression $f(n)$ so that $C_{n+1} = f(n)C_n$. Use this to compute $C_1, \ldots, C_6$ from C_0.

3. Show that if A_n is the number of properly matched sequences of parentheses of length $2n$, then

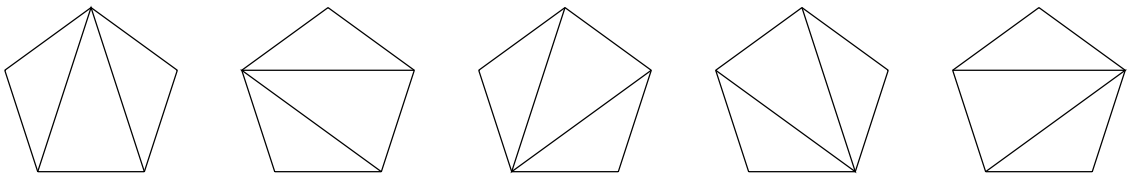
$$A_n = \sum_{i=0}^{n-1} A_i A_{n-i-1}.$$

Do this in the same style that we used for the number of rooted binary trees: Given all the sequences of shorter length, explain how to combine them to produce the sequences of length $2n$, in such a way that the sum clearly counts the number of sequences. Hint: Prove the following lemma: If s is a properly matched sequence of parentheses of length $2n$, s may be written uniquely in the form $(s_1)s_2$, where s_1 and s_2 are properly matched sequences of parentheses whose lengths add to $2n-2$. For example, (())() = ([()])[()] and ()(()) = ([])[(())], with the sequences s_1 and s_2 indicated by [ ]. Note that s_1 and s_2 are allowed to be empty sequences, with length 0.

4. Consider a "staircase" as shown below. A path from A to B consists of a sequence of edges starting at A, ending at B, and proceeding only up or right; all paths are of length 6. One such path is indicated by arrows. The staircase shown is a "3×3" staircase. How many paths are there in an $n \times n$ staircase?



5. A convex polygon with $n \geq 3$ sides can be divided into triangles by inserting $n-3$ non-intersecting diagonals. In how many different ways can this be done? The possibilities for $n = 5$ are shown.



6. A **partition** of a set S is a collection of non-empty subsets $A_i \subseteq S$, $1 \leq i \leq k$ (the **parts** of the partition), such that $\bigcup_{i=1}^{k} A_i = S$ and for every $i \neq j$, $A_i \cap A_j = \emptyset$. For example, one partition of $\{1,2,3,4,5\}$ is $\{\{1,3\}, \{4\}, \{2,5\}\}$.

Suppose the integers $1, 2, \ldots, n$ are arranged on a circle, in order around the circle. A partition of $\{1, 2, \ldots, n\}$ is a **non-crossing partition** if it satisfies this additional property: If w and x are in some part A_i, and y and z are in a different part A_j, then the line joining w to x does not cross the line joining y to z. The partition above, $\{1,3\}$, $\{4\}$, $\{2,5\}$, is not a non-crossing partition, as the the line 1–3 crosses the line 2–5.

Find the number of non-crossing partitions of $\{1, 2, \ldots, n\}$.

Recall from section 1.4 that the Bell numbers count all of the partitions of $\{1, 2, \ldots, n\}$. Hence, this exercise gives us a lower bound on the total number of partitions.

7. Consider a set of $2n$ people sitting around a table. In how many ways can we arrange for each person to shake hands with another person at the table such that no two handshakes cross?

4

Systems of Distinct Representatives

Suppose that the student clubs at a college each send a representative to the student government from among the members of the club. No person may represent more than one club; is this possible? It is certainly possible sometimes, for example when no student belongs to two clubs. It is not hard to see that it could be impossible. So the first substantive question is: is there anything useful or interesting we can say about under what conditions it is possible to choose such representatives.

We turn this into a more mathematical situation:

DEFINITION 4.0.1 Suppose that $A_1, A_2, \ldots, A_n$ are sets, which we refer to as a **set system**. A (complete) **system of distinct representatives** is a sequence $\{x_1, x_2, \ldots x_n\}$ such that $x_i \in A_i$ for all i, and no two of the x_i are the same. A (partial) system of distinct representatives is a sequence of distinct elements $\{x_1, x_2, \ldots x_k\}$ such that $x_i \in A_{j_i}$, where $j_1, j_2, \ldots, j_k$ are distinct integers in $[n]$. □

In standard usage, "system of distinct representatives" means "complete system of distinct representatives", but it will be convenient to let "system of distinct representatives" mean either a complete or partial system of distinct representatives depending on context. We usually abbreviate "system of distinct representatives" as SDR.

We will analyze this problem in two ways, combinatorially and using graph theory.

4.1 Existence of SDRs

In this section, SDR means complete SDR. It is easy to see that not every collection of sets has an SDR. For example,

$$A_1 = \{a, b\}, A_2 = \{a, b\}, A_3 = \{a, b\}.$$

The problem is clear: there are only two possible representatives, so a set of three distinct representatives cannot be found. This example is a bit more general than it may at first appear. Consider

$$A_1 = \{a, b\}, A_2 = \{a, b\}, A_3 = \{a, b\}, A_4 = \{b, c, d, e\}.$$

Now the total number of possible representatives is 5, and we only need 4. Nevertheless, this is impossible, because the first three sets have no SDR considered by themselves. Thus the following condition, called **Hall's Condition**, is clearly necessary for the existence of an SDR: For every $k \geq 1$, and every set $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$, $|\bigcup_{j=1}^{k} A_{i_j}| \geq k$. That is, the number of possible representatives in any collection of sets must be at least as large as the number of sets. Both examples fail to have this property because $|A_1 \cup A_2 \cup A_3| = 2 < 3$.

Remarkably, this condition is both necessary and sufficient.

THEOREM 4.1.1 Hall's Theorem A collection of sets $A_1, A_2, \ldots, A_n$ has an SDR if and only if for every $k \geq 1$, and every set $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$, $|\bigcup_{j=1}^{k} A_{i_j}| \geq k$.

Proof. We already know the condition is necessary, so we prove sufficiency by induction on n.

Suppose $n = 1$; the condition is simply that $|A_1| \geq 1$. If this is true then A_1 is non-empty and so there is an SDR. This establishes the base case.

Now suppose that the theorem is true for a collection of $k < n$ sets, and suppose we have sets $A_1, A_2, \ldots, A_n$ satisfying Hall's Condition. We need to show there is an SDR.

Suppose first that for every $k < n$ and every $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$, that $|\bigcup_{j=1}^{k} A_{i_j}| \geq k + 1$, that is, that these unions are larger than required. Pick any element $x_n \in A_n$, and define $B_i = A_i \backslash \{x_n\}$ for each $i < n$. Consider the collection of sets $B_1, \ldots, B_{n-1}$, and any union $\bigcup_{j=1}^{k} B_{i_j}$ of a subcollection of the sets. There are two possibilities: either $\bigcup_{j=1}^{k} B_{i_j} = \bigcup_{j=1}^{k} A_{i_j}$ or $\bigcup_{j=1}^{k} B_{i_j} = \bigcup_{j=1}^{k} A_{i_j} \backslash \{x_n\}$, so that $|\bigcup_{j=1}^{k} B_{i_j}| = |\bigcup_{j=1}^{k} A_{i_j}|$ or $|\bigcup_{j=1}^{k} B_{i_j}| = |\bigcup_{j=1}^{k} A_{i_j}| - 1$. In either case, since $|\bigcup_{j=1}^{k} A_{i_j}| \geq k+1$, $|\bigcup_{j=1}^{k} B_{i_j}| \geq k$. Thus, by the induction hypothesis, the collection $B_1, \ldots, B_{n-1}$ has an SDR $\{x_1, x_2, \ldots, x_{n-1}\}$, and for every $i < n$, $x_i \neq x_n$, by the definition of the B_i. Thus $\{x_1, x_2, \ldots, x_n\}$ is an SDR for $A_1, A_2, \ldots, A_n$.

If it is not true that for every $k < n$ and every $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$, $|\bigcup_{j=1}^{k} A_{i_j}| \geq k+1$, then for some $k < n$ and $\{i_1, i_2, \ldots, i_k\}$, $|\bigcup_{j=1}^{k} A_{i_j}| = k$. Without loss of generality, we

may assume that $|\bigcup_{j=1}^{k} A_j| = k$. By the induction hypothesis, $A_1, A_2, \ldots, A_k$ has an SDR, $\{x_1, \ldots, x_k\}$.

Define $B_i = A_i \backslash \bigcup_{j=1}^{k} A_j$ for $i > k$. Suppose that $\{x_{k+1}, \ldots, x_n\}$ is an SDR for $B_{k+1}, \ldots, B_n$; then it is also an SDR for $A_{k+1}, \ldots, A_n$. Moreover, $\{x_1, \ldots, x_n\}$ is an SDR for $A_1, \ldots, A_n$. Thus, to finish the proof it suffices to show that $B_{k+1}, \ldots, B_n$ has an SDR. The number of sets here is $n - k < n$, so we need only show that the sets satisfy Hall's Condition.

So consider some sets $B_{i_1}, B_{i_2}, \ldots, B_{i_l}$. First we notice that

$$|A_1 \cup A_2 \cup \cdots \cup A_k \cup B_{i_1} \cup B_{i_2} \cup \cdots B_{i_l}| = k + |B_{i_1} \cup B_{i_2} \cup \cdots B_{i_l}|.$$

Also

$$|A_1 \cup A_2 \cup \cdots \cup A_k \cup B_{i_1} \cup B_{i_2} \cup \cdots B_{i_l}| = |A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{i_1} \cup A_{i_2} \cup \cdots A_{i_l}|$$

and

$$|A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{i_1} \cup A_{i_2} \cup \cdots A_{i_l}| \geq k + l.$$

Putting these together gives

$$\begin{aligned} k + |B_{i_1} \cup B_{i_2} \cup \cdots \cup B_{i_l}| &\geq k + l \\ |B_{i_1} \cup B_{i_2} \cup \cdots \cup B_{i_l}| &\geq l \\ &. \end{aligned}$$

Thus, $B_{k+1}, \ldots, B_n$ has an SDR, which finishes the proof. ∎

Exercises 4.1.

1. How many different systems of distinct representatives are there for $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $\ldots$, $A_n = \{n, 1\}$?
2. How many different systems of distinct representatives are there for the sets $A_i = [n] \backslash i$, $i = 1, 2, \ldots, n$, $n \geq 2$?
3. Suppose the set system $A_1, A_2, \ldots, A_n$ has an SDR, and that $x \in A_i$. Show the set system has an SDR containing x. Show that x cannot necessarily be chosen to represent A_i.
4. Suppose the set system $A_1, A_2, \ldots, A_n$ satisfies $|\bigcup_{j=1}^{k} A_{i_j}| \geq k + 1$ for every $1 \leq k < n$ and $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$, and that $x \in A_i$. Show the set system has an SDR in which x represents A_i.
5. An $m \times n$ chessboard, with m even and both m and n at least 2, has one white and one black square removed. Show that the board can be covered by dominoes.

4.2 Partial SDRs

In this section, SDR means partial SDR.

If there is no complete SDR, we naturally want to know how many of the n sets can be represented, that is, what is the largest value of m so that some m of the sets have a complete SDR. Since there is no complete SDR, there are sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ such that $|\bigcup_{j=1}^{k} A_{i_j}| = l < k$. Clearly at most l of these k sets have a complete SDR, so no SDR for $A_1, A_2, \ldots, A_n$ can be larger than $n - k + l$. Thus, m can be no larger than the minimum value, over all k and all collections of sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, of $n-k+|\bigcup_{j=1}^{k} A_{i_j}|$. Note that if $|\bigcup_{j=1}^{k} A_{i_j}| > k$, $n - k + |\bigcup_{j=1}^{k} A_{i_j}| > n$, which tells us nothing. If $k = 0$, $n - k + |\bigcup_{j=1}^{k} A_{i_j}| = n$ (because empty unions are empty), so we are guaranteed that the minimum is never greater than n. In fact the minimum value of the expression is exactly the size of a largest SDR.

THEOREM 4.2.1 The maximum size of an SDR for the sets $A_1, A_2, \ldots, A_n$ is the minimum value, for $0 \le k \le n$ and sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, of $n - k + |\bigcup_{j=1}^{k} A_{i_j}|$.

Proof. Since no SDR can be larger than this minimum value, it suffices to show that we can find an SDR whose size is this minimum. The proof is by induction on n; the case $n = 1$ is easy.

Suppose first that the minimum value is n, so that for all k and all collections of sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$,

$$n - k + |\bigcup_{j=1}^{k} A_{i_j}| \ge n.$$

Then rearranging we see that

$$|\bigcup_{j=1}^{k} A_{i_j}| \ge k,$$

so by Hall's Theorem (4.1.1), there is an SDR of size n.

Note that the minimum value of $n - k + |\bigcup_{j=1}^{k} A_{i_j}|$ occurs when $|\bigcup_{j=1}^{k} A_{i_j}| - k$ is a minimum, that is

$$\min(n - k + |\bigcup_{j=1}^{k} A_{i_j}|) = n + \min(|\bigcup_{j=1}^{k} A_{i_j}| - k).$$

Suppose now that the minimum m is less than n, and that $m = n - k + |\bigcup_{j=1}^{k} A_{i_j}|$, with $0 < k < n$. Let $B_j = A_{i_j}$; since $k < n$, the induction hypothesis applies to the sets $B_1, \ldots, B_k$. Since each set B_j is A_{i_j}, $|\bigcup_{j=1}^{l} B_{h_j}| - l \ge |\bigcup_{j=1}^{k} A_{i_j}| - k$, for all l and $B_{h_1}, \ldots, B_{h_l}$. Thus, the minimum value of $|\bigcup_{j=1}^{l} B_{i_j}| - l$, over all l and $B_{h_1}, \ldots, B_{h_l}$, is

$|\bigcup_{j=1}^{k} B_j| - k = |\bigcup_{j=1}^{k} A_{i_j}| - k$, so by the induction hypothesis, the sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ have an SDR of size $k - k + |\bigcup_{j=1}^{k} A_{i_j}| = |\bigcup_{j=1}^{k} A_{i_j}| = m - n + k$, $\{x_1, \ldots, x_{m-n+k}\}$.

Now consider the $n - k$ sets consisting of those original sets not in $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, that is, $\{A_i \mid i \notin \{i_1, \ldots, i_k\}\}$. Let $C_i = A_i \setminus \bigcup_{j=1}^{k} A_{i_j}$ for i not in $i_1, i_2, \ldots, i_k$. Consider some sets $C_{g_1}, C_{g_2}, \ldots, C_{g_l}$. If $|\bigcup_{j=1}^{l} C_{g_j}| < l$ then $|\bigcup_{j=1}^{l} C_{g_j}| - l < 0$ and

$$\begin{aligned} n - k + |\bigcup_{j=1}^{k} A_{i_j}| &> n - k - l + |\bigcup_{j=1}^{l} C_{g_j}| + |\bigcup_{j=1}^{k} A_{i_j}| \\ &\geq n - (k + l) + |C_{g_1} \cup \cdots \cup C_{g_l} \cup A_{i_1} \cup \cdots \cup A_{i_k}| \\ &= n - (k + l) + |A_{g_1} \cup \cdots \cup A_{g_l} \cup A_{i_1} \cup \cdots \cup A_{i_k}|, \end{aligned}$$

contradicting the fact that $n-k+|\bigcup_{j=1}^{k} A_{i_j}|$ is a minimum. Thus by Hall's Theorem (4.1.1), the sets $C_{g_1}, C_{g_2}, \ldots, C_{g_{n-k}}$ have a complete SDR $\{y_1, \ldots, y_{n-k}\}$. By the definition of the sets C_i, $\{x_1, \ldots, x_{m-n+k}\} \cap \{y_1, \ldots, y_{n-k}\} = \emptyset$, so $\{x_1, \ldots, x_{m-n+k}\} \cup \{y_1, \ldots, y_{n-k}\}$ is an SDR of size $m - n + k + n - k = m$ as desired.

Finally, suppose that the minimum value of $n-k+|\bigcup_{j=1}^{k} A_{i_j}|$ occurs only when $k = n$, so we want an SDR of size

$$n - n + |\bigcup_{j=1}^{n} A_j| = |\bigcup_{j=1}^{n} A_j|.$$

Then

$$\begin{aligned} n - (n-1) + |\bigcup_{j=1}^{n-1} A_j| &> |\bigcup_{j=1}^{n} A_j| \\ 1 + |\bigcup_{j=1}^{n-1} A_j| &> |\bigcup_{j=1}^{n} A_j| \\ |\bigcup_{j=1}^{n-1} A_j| &\geq |\bigcup_{j=1}^{n} A_j|. \end{aligned}$$

Since $|\bigcup_{j=1}^{n-1} A_j| \leq |\bigcup_{j=1}^{n} A_j|$, $|\bigcup_{j=1}^{n-1} A_j| = |\bigcup_{j=1}^{n} A_j|$. By the induction hypothesis, the theorem applies to the sets $A_1, A_2, \ldots, A_{n-1}$. If the minimum of $(n-1) - l + |\bigcup_{j=1}^{l} A_{i_j}|$ occurs when $l = n - 1$, then there is an SDR of size $(n-1) - (n-1) + |\bigcup_{j=1}^{n-1} A_j| = |\bigcup_{j=1}^{n-1} A_j| = |\bigcup_{j=1}^{n} A_j|$, as desired.

If the minimum occurs when $l < n - 1$ and not when $l = n - 1$, then

$$\begin{aligned} (n-1) - l + |\bigcup_{j=1}^{l} A_{i_j}| &< |\bigcup_{j=1}^{n-1} A_j| \\ n - l + |\bigcup_{j=1}^{l} A_{i_j}| &< |\bigcup_{j=1}^{n-1} A_j| + 1 \end{aligned}$$

and by assumption

$$n - l + |\bigcup_{j=1}^{l} A_{i_j}| > |\bigcup_{j=1}^{n} A_j|.$$

Thus

$$\begin{aligned} |\bigcup_{j=1}^{n} A_j| &< n - l + |\bigcup_{j=1}^{l} A_{i_j}| \\ &< |\bigcup_{j=1}^{n-1} A_j| + 1 \\ &= |\bigcup_{j=1}^{n} A_j| + 1. \end{aligned}$$

This means that there is an integer strictly between two consecutive integers, a contradiction. This completes the proof. ■

While this theorem provides a method to calculate the size of a maximum SDR, the method is hardly efficient: it requires looking at all possible collections of the sets. It also does not provide a way to find an actual SDR, that is, the actual representatives. We will fix these problems in the last two sections of this chapter.

Exercises 4.2.

1. Find the size of a maximum SDR for

$$A_1 = \{a, b, c\}, A_2 = \{a, b, c, d, e\}, A_3 = \{a, b\}, A_4 = \{b, c\}, A_5 = \{a\}, A_6 = \{a, c, e\}.$$

Justify your answer.

4.3 Latin Squares

DEFINITION 4.3.1 A **Latin square** of order n is an $n \times n$ grid filled with n symbols so that each symbol appears once in each row and column. □

EXAMPLE 4.3.2 Here is a Latin square of order 4:

♡	♣	♠	♢
♣	♠	♢	♡
♠	♢	♡	♣
♢	♡	♣	♠

□

Usually we use the integers $1 \ldots n$ for the symbols. There are many, many Latin squares of order n, so it pays to limit the number by agreeing not to count Latin squares

that are "really the same" as different. The simplest way to do this is to consider **reduced** Latin squares. A reduced Latin square is one in which the first row is $1 \ldots n$ (in order) and the first column is likewise $1 \ldots n$.

EXAMPLE 4.3.3 Consider this Latin square:

4	2	3	1
2	4	1	3
1	3	4	2
3	1	2	4

The order of the rows and columns is not really important to the idea of a Latin square. If we reorder the rows and columns, we can consider the result to be in essence the same Latin square. By reordering the columns, we can turn the square above into this:

1	2	3	4
3	4	1	2
2	3	4	1
4	1	2	3

Then we can swap rows two and three:

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

This Latin square is in reduced form, and is essentially the same as the original. □

Another simple way to change the appearance of a Latin square without changing its essential structure is to interchange the symbols.

EXAMPLE 4.3.4 Starting with the same Latin square as before:

4	2	3	1
2	4	1	3
1	3	4	2
3	1	2	4

we can interchange the symbols 1 and 4 to get:

1	2	3	4
2	1	4	3
4	3	1	2
3	4	2	1

Now if we swap rows three and four we get:

1	2	3	4
2	1	4	3
3	4	2	1
4	3	1	2

Notice that this Latin square is in reduced form, but it is not the same as the reduced form from the previous example, even though we started with the same Latin square. Thus, we may want to consider some reduced Latin squares to be the same as each other. □

DEFINITION 4.3.5 Two Latin squares are **isotopic** if each can be turned into the other by permuting the rows, columns, and symbols. This isotopy relation is an equivalence relation; the equivalence classes are the **isotopy classes**. □

Latin squares are apparently quite difficult to count without substantial computing power. According to Wikipedia, the number of Latin squares is known only up to $n = 11$. Here are the first few values for all Latin squares, reduced Latin squares, and non-isotopic Latin squares (that is, the number of isotopy classes):

n	All	Reduced	Non-isotopic
1	1	1	1
2	2	1	1
3	12	1	1
4	576	4	2
5	161280	56	2

How can we produce a Latin square? If you know what a group is, you should know that the multiplication table of any finite group is a Latin square. (Also, any Latin square is the multiplication table of a **quasigroup**.) Even if you have not encountered groups by that name, you may know of some. For example, considering the integers modulo n under addition, the addition table is a Latin square.

EXAMPLE 4.3.6 Here is the addition table for the integers modulo 6:

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

□

EXAMPLE 4.3.7 Here is another way to potentially generate many Latin squares. Start with first row $1, \ldots, n$. Consider the sets $A_i = [n] \backslash \{i\}$. From exercise 1 in section 4.1 we know that this set system has many SDRs; if $x_1, x_2, \ldots, x_n$ is an SDR, we may use it for row two. In general, after we have chosen rows $1, \ldots, j$, we let A_i be the set of integers that have not yet been chosen for column i. This set system has an SDR, which we use for row $j + 1$. □

DEFINITION 4.3.8 Suppose A and B are two Latin squares of order n, with entries $A_{i,j}$ and $B_{i,j}$ in row i and column j. Form the matrix M with entries $M_{i,j} = (A_{i,j}, B_{i,j})$; we will denote this operation as $M = A \cup B$. We say that A and B are **orthogonal** if M contains all n^2 ordered pairs (a, b), $1 \leq a \leq n$, $1 \leq b \leq n$, that is, all elements of $\{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$. □

As we will see, it is easy to find orthogonal Latin squares of order n if n is odd; not too hard to find orthogonal Latin squares of order $4k$, and difficult but possible to find orthogonal Latin squares of order $4k+2$, with the exception of orders 2 and 6. In the 1700s, Euler showed that there are orthogonal Latin squares of all orders except of order $4k + 2$, and he conjectured that there are no orthogonal Latin squares of of order 6. In 1901, the amateur mathematician Gaston Tarry showed that indeed there are none of order 6, by showing that all possibilities for such Latin squares failed to be orthogonal. In 1959 it was finally shown that there are orthogonal Latin squares of all other orders.

THEOREM 4.3.9 There are pairs of orthogonal Latin squares of order n when n is odd.

Proof. This proof can be shortened by using ideas of group theory, but we will present a self-contained version. Consider the addition table for addition mod n:

	0	$\cdots$	j	$\cdots$	$n-1$
0	0	$\cdots$	j	$\cdots$	$n-1$
$\vdots$					
i	i	$\cdots$	$i+j$	$\cdots$	$n+i-1$
$\vdots$					
$n-1$	$n-1$	$\cdots$	$n+j-1$	$\cdots$	$n-2$

We claim first that this (without the first row and column, of course) is a Latin square with symbols $0, 1, \ldots, n-1$. Consider two entries in row i, say $i+j$ and $i+k$. If $i+j \equiv i+j \pmod{n}$, then $j \equiv k$, so $j = k$. Thus, all entries of row i are distinct, so each of $0, 1, \ldots, n-1$ appears exactly once in row i. The proof that each appears once in any column is similar. Call this Latin square A. (Note that so far everything is true whether n is odd or even.)

Now form a new square B with entries $B_{i,j} = A_{2i,j} = 2i + j$, where by $2i$ and $2i + j$ we mean those values mod n. Thus row i of B is the same as row $2i$ of A. Now we claim that in fact the rows of B are exactly the rows of A, in a different order. To do this, it suffices to show that if $2i \equiv 2k \pmod{n}$, then $i = k$. This implies that all the rows of B are distinct, and hence must be all the rows of A.

Suppose without loss of generality that $i \geq k$. If $2i \equiv 2k \pmod{n}$ then $n \mid 2(i-k)$. Since n is odd, $n \mid (i-k)$. Since i and k are in $0, 1, \ldots, n-1$, $0 \leq i-k \leq n-1$. Of these values, only 0 is divisible by n, so $i - k = 0$. Thus B is also a Latin square.

To show that $A \cup B$ contains all n^2 elements of $\{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$, it suffices to show that no two elements of $A \cup B$ are the same. Suppose that $(i_1 + j_1, 2i_1 + j_1) = (i_2 + j_2, 2i_2 + j_2)$ (arithmetic is mod n). Then by subtracting equations, $i_1 = i_2$; with the first equation this implies $j_1 = j_2$. ■

EXAMPLE 4.3.10 When $n = 3$,

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \cup \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{bmatrix}.$$

□

One obvious approach to constructing Latin squares, and pairs of orthogonal Latin squares, is to start with smaller Latin squares and use them to produce larger ones. We will produce a Latin square of order mn from a Latin square of order m and one of order n.

Let A be a Latin square of order m with symbols $1, \ldots, m$, and B one of order n with symbols $1, \ldots, n$. Let $c_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n$, be mn new symbols. Form an $mn \times mn$ grid by replacing each entry of B with a copy of A. Then replace each entry i in this copy

of A with $c_{i,j}$, where j is the entry of B that was replaced. We denote this new Latin square $A \times B$. Here is an example, combining a 4×4 Latin square with a 3×3 Latin square to form a 12×12 Latin square:

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

$\times$

1	2	3
2	3	1
3	1	2

$=$

$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$
$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{1,1}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{1,2}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{1,3}$
$c_{3,1}$	$c_{4,1}$	$c_{1,1}$	$c_{2,1}$	$c_{3,2}$	$c_{4,2}$	$c_{1,2}$	$c_{2,2}$	$c_{3,3}$	$c_{4,3}$	$c_{1,3}$	$c_{2,3}$
$c_{4,1}$	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,2}$	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,3}$	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$
$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$
$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{1,2}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{1,3}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{1,1}$
$c_{3,2}$	$c_{4,2}$	$c_{1,2}$	$c_{2,2}$	$c_{3,3}$	$c_{4,3}$	$c_{1,3}$	$c_{2,3}$	$c_{3,1}$	$c_{4,1}$	$c_{1,1}$	$c_{2,1}$
$c_{4,2}$	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,3}$	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,1}$	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$
$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$
$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{1,3}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{1,1}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{1,2}$
$c_{3,3}$	$c_{4,3}$	$c_{1,3}$	$c_{2,3}$	$c_{3,1}$	$c_{4,1}$	$c_{1,1}$	$c_{2,1}$	$c_{3,2}$	$c_{4,2}$	$c_{1,2}$	$c_{2,2}$
$c_{4,3}$	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,1}$	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,2}$	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$

THEOREM 4.3.11 If A and B are Latin squares, so is $A \times B$.

Proof. Consider two symbols $c_{i,j}$ and $c_{k,l}$ in the same row. If the positions containing these symbols are in the same copy of A, then $i \neq k$, since A is a Latin square, and so the symbols $c_{i,j}$ and $c_{k,l}$ are distinct. Otherwise, $j \neq l$, since B is a Latin square. The argument is the same for columns. ■

Remarkably, this operation preserves orthogonality:

THEOREM 4.3.12 If A_1 and A_2 are Latin squares of order m, B_1 and B_2 are Latin squares of order n, A_1 and A_2 are orthogonal, and B_1 and B_2 are orthogonal, then $A_1 \times B_1$ is orthogonal to $A_1 \times B_2$.

Proof. We denote the contents of $A_i \times B_i$ by $C_i(w, x, y, z)$, meaning the entry in row w and column x of the copy of A_i that replaced the entry in row y and column z of B_i, which we denote $B_i(y, z)$. We use $A_i(w, x)$ to denote the entry in row w and column x of A_i.

Suppose that $(C_1(w, x, y, z), C_2(w, x, y, z)) = (C_1(w', x', y', z'), C_2(w', x', y', z'))$, where $(w, x, y, z) \neq (w', x', y', z')$. Either $(w, x) \neq (w', x')$ or $(y, z) \neq (y', z')$. If the latter, then $(B_1(y, z), B_2(y, z)) = (B_1(y', z'), B_2(y', z'))$, a contradiction, since B_1 is orthogonal to B_2. Hence $(y, z) = (y', z')$ and $(w, x) \neq (w', x')$. But this implies that $(A_1(w, x), A_2(w, x)) = (A_1(w', x'), A_2(w', x'))$, a contradiction. Hence $A_1 \times B_1$ is orthogonal to $A_1 \times B_2$. ■

We want to construct orthogonal Latin squares of order $4k$. Write $4k = 2^m \cdot n$, where n is odd and $m \geq 2$. We know there are orthogonal Latin squares of order n, by theorem 4.3.9. If there are orthogonal Latin squares of order 2^m, then by theorem 4.3.12 we can construct orthogonal Latin squares of order $4k = 2^m \cdot n$.

To get a Latin square of order 2^m, we also use theorem 4.3.12. It suffices to find two orthogonal Latin squares of order $4 = 2^2$ and two of order $8 = 2^3$. Then repeated application of theorem 4.3.12 allows us to build orthogonal Latin squares of order 2^m, $m \geq 2$.

Two orthogonal Latin squares of order 4:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix},$$

and two of order 8:

$$\begin{bmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\ 5 & 2 & 7 & 1 & 8 & 4 & 6 & 3 \\ 6 & 4 & 3 & 8 & 1 & 2 & 5 & 7 \\ 7 & 8 & 5 & 4 & 2 & 1 & 3 & 6 \\ 8 & 7 & 2 & 6 & 5 & 3 & 1 & 4 \\ 2 & 5 & 8 & 3 & 7 & 6 & 4 & 1 \\ 3 & 1 & 6 & 2 & 4 & 8 & 7 & 5 \\ 4 & 6 & 1 & 7 & 3 & 5 & 2 & 8 \end{bmatrix} \begin{bmatrix} 1 & 4 & 5 & 6 & 7 & 8 & 2 & 3 \\ 8 & 2 & 6 & 5 & 3 & 1 & 4 & 7 \\ 2 & 8 & 3 & 7 & 6 & 4 & 1 & 5 \\ 3 & 6 & 2 & 4 & 8 & 7 & 5 & 1 \\ 4 & 1 & 7 & 3 & 5 & 2 & 8 & 6 \\ 5 & 7 & 1 & 8 & 4 & 6 & 3 & 2 \\ 6 & 3 & 8 & 1 & 2 & 5 & 7 & 4 \\ 7 & 5 & 4 & 2 & 1 & 3 & 6 & 8 \end{bmatrix}.$$

Exercises 4.3.

1. Show that there is only one reduced Latin square of order 3.
2. Verify that the isotopy relation is an equivalence relation.
3. Find all 4 reduced Latin squares of order 4. Show that there are at most 2 isotopy classes for order 4.
4. Show that the second set system defined in example 4.3.7 has an SDR as claimed.
5. Show that there are no orthogonal Latin squares of order 2.
6. Find the two orthogonal Latin squares of order 5 as described in theorem 4.3.9. Show your answer as in example 4.3.10.
7. Prove that to construct orthogonal Latin squares of order 2^m, $m \geq 2$, it suffices to find two orthogonal Latin squares of order $4 = 2^2$ and two of order $8 = 2^3$.
8. An $n \times n$ Latin square A is **symmetric** if it is symmetric around the main diagonal, that is, $A_{i,j} = A_{j,i}$ for all i and j. It is easy to find symmetric Latin squares: every addition table modulo n is an example, as in example 4.3.6. A Latin square is **idempotent** if every symbol appears on the main diagonal. Show that if A is both symmetric and idempotent, then n is odd. Find a 5×5 symmetric, idempotent Latin square.

9. The **transpose** $A^\top$ of a Latin square A is the reflection of A across the main diagonal, so that $A^\top_{i,j} = A_{j,i}$. A Latin square is self-orthogonal if A is orthogonal to $A^\top$. Show that there is no self-orthogonal Latin square of order 3. Find one of order 4.

4.4 Introduction to Graph Theory

We can interpret the SDR problem as a problem about graphs. Given sets $A_1, A_2, \ldots, A_n$, with $\bigcup_{i=1}^n A_i = \{x_1, x_2, \ldots, x_m\}$, we define a graph with $n+m$ vertices as follows: The vertices are labeled $\{A_1, A_2, \ldots, A_n, x_1, x_2, \ldots x_m\}$, and the edges are $\{\{A_i, x_j\} \mid x_j \in A_i\}$.

EXAMPLE 4.4.1 Let $A_1 = \{a, b, c, d\}$, $A_2 = \{a, c, e, g\}$, $A_3 = \{b, d\}$, and $A_4 = \{a, f, g\}$. The corresponding graph is shown in figure 4.4.1. □

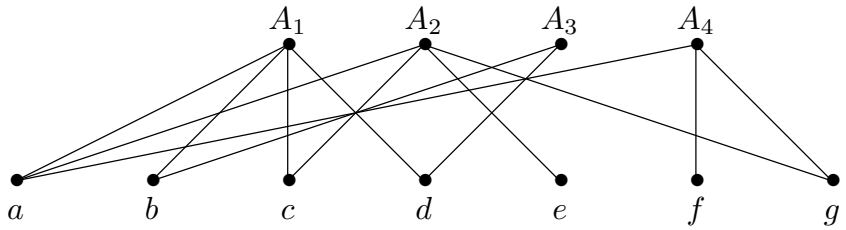


Figure 4.4.1 A set system depicted as a bipartite graph.

Before exploring this idea, we introduce a few basic concepts about graphs. If two vertices in a graph are connected by an edge, we say the vertices are **adjacent**. If a vertex v is an endpoint of edge e, we say they are **incident**. The set of vertices adjacent to v is called the **neighborhood** of v, denoted $N(v)$. This is sometimes called the **open neighborhood** of v to distinguish it from the **closed neighborhood** of v, $N[v] = N(v) \cup \{v\}$. The **degree** of a vertex v is the number of edges incident with v; it is denoted $\mathrm{d}(v)$.

Some simple types of graph come up often: A **path** is a graph P_n on vertices $v_1, v_2, \ldots, v_n$, with edges $\{v_i, v_{i+1}\}$ for $1 \le i \le n-1$, and no other edges. A **cycle** is a graph C_n on vertices $v_1, v_2, \ldots, v_n$ with edges $\{v_i, v_{1+(i \bmod n)}\}$ for $1 \le i \le n$, and no other edges; this is a path in which the first and last vertices have been joined by an edge. (Generally, we require that a cycle have at least three vertices. If it has two, then the two are joined by two distinct edges; when a graph has more than one edge with the same endpoints it is called a **multigraph**. If a cycle has one vertex, there is an edge, called a **loop**, in which a single vertex serves as both endpoints.) The **length** of a path or cycle is the number of edges in the graph. For example, P_1 has length 0, C_1 has length 1. A **complete graph** K_n is a graph on $v_1, v_2, \ldots, v_n$ in which every two distinct vertices are joined by an edge. See figure 4.4.2 for examples.

The graph in figure 4.4.1 is a **bipartite graph**.

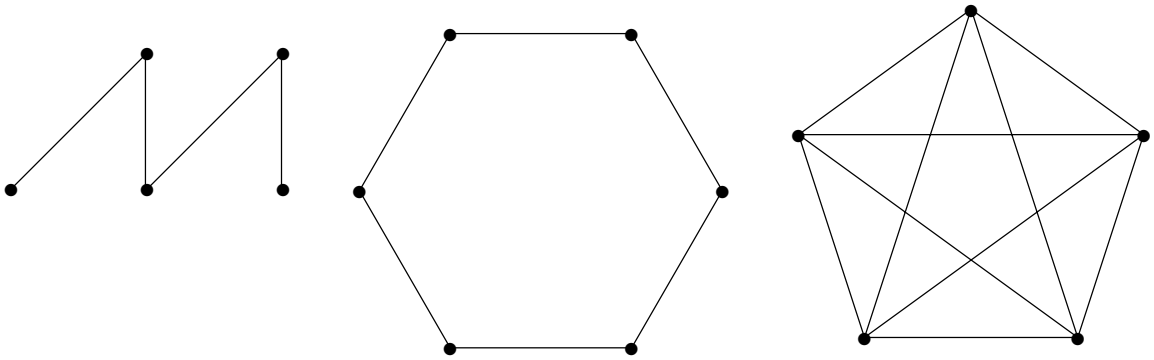


Figure 4.4.2 Graphs P_5, C_6, K_5.

DEFINITION 4.4.2 A graph G is bipartite if its vertices can be partitioned into two parts, say $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_m\}$ so that all edges join some v_i to some w_j; no two vertices v_i and v_j are adjacent, nor are any vertices w_i and w_j. □

The graph in figure 4.4.1 is bipartite, as are the first two graphs in figure 4.4.2.

4.5 Matchings

Now we return to systems of distinct representatives.

A system of distinct representatives corresponds to a set of edges in the corresponding bipartite graph that share no endpoints; such a collection of edges (in any graph, not just a bipartite graph) is called a **matching**. In figure 4.5.1, a matching is shown in red. This is a largest possible matching, since it contains edges incident with all four of the top vertices, and it thus corresponds to a complete SDR.

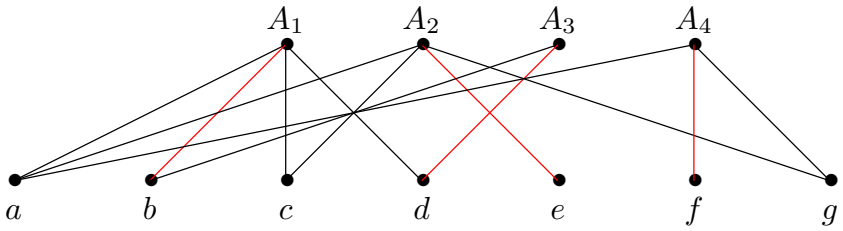


Figure 4.5.1 A set system depicted as a bipartite graph.

Any bipartite graph can be interpreted as a set system: we simply label all the vertices in one part with "set names" A_1, A_2, etc., and the other part is labeled with "element names", and the sets are defined in the obvious way: A_i is the neighborhood of the vertex labeled "A_i". Thus, we know one way to compute the size of a maximum matching, namely, we interpret the bipartite graph as a set system and compute the size of a maximum SDR; this is the size of a maximum matching.

We will see another way to do this working directly with the graph. There are two advantages to this: it will turn out to be more efficient, and as a by-product it will actually find a maximum matching.

Given a bipartite graph, it is easy to find a *maximal* matching, that is, one that cannot be made larger simply by adding an edge: just choose edges that do not share endpoints until this is no longer possible. See figure 4.5.2 for an example.

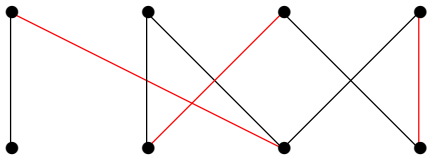


Figure 4.5.2 A maximal matching is shown in red.

An obvious approach is then to attempt to make the matching larger. There is a simple way to do this, if it works: We look for an **alternating chain**, defined as follows.

DEFINITION 4.5.1 Suppose M is a matching, and suppose that $v_1, w_1, v_2, w_2, \ldots, v_k, w_k$ is a sequence of vertices such that no edge in M is incident with v_1 or w_k, and moreover for all $1 \leq i \leq k$, v_i and w_i are joined by an edge not in M, and for all $1 \leq i \leq k-1$, w_i and v_{i+1} are joined by an edge in M. Then the sequence of vertices together with the edges joining them in order is an alternating chain. □

The graph in figure 4.5.2 contains alternating chains, one of which is shown in figure 4.5.3.

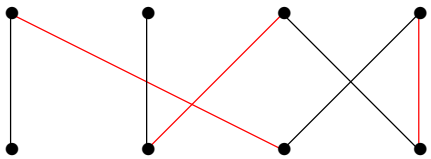


Figure 4.5.3 An alternating chain.

Suppose now that we remove from M all the edges that are in the alternating chain and also in M, forming M', and add to M' all of the edges in the alternating chain not in M, forming M''. It is not hard to show that M'' is a matching, and it contains one more edge than M. See figure 4.5.4.

Remarkably, if there is no alternating chain, then the matching M is a maximum matching.

THEOREM 4.5.2 Suppose that M is a matching in a bipartite graph G, and there is no alternating chain. Then M is a maximum matching.

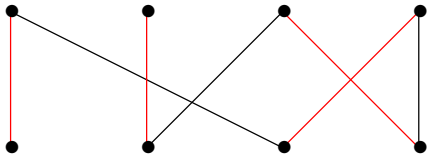


Figure 4.5.4 A new, larger matching.

Proof. We prove the contrapositive: Suppose that M is not a maximum matching. Then there is a larger matching, N. Create a new graph G' by eliminating all edges that are in both M and N, and also all edges that are in neither. We are left with just those edges in M or N but not both.

In this new graph no vertex is incident with more than two edges, since if v were incident with three edges, at least two of them would belong to M or two would belong to N, but that can't be true since M and N are matchings. This means that G' is composed of disjoint paths and cycles. Since N is larger than M, G' contains more edges from N than from M, and therefore one of the paths starts and ends with an edge from N, and along the path the edges alternate between edges in N and edges in M. In the original graph G with matching M, this path forms an alternating chain. The "alternating" part is clear; we need to see that the first and last vertices in the path are not incident with any edge in M.

Suppose that the first two vertices are v_1 and v_2. Then v_1 and v_2 are joined by an edge of N. Suppose that v_1 is adjacent to a vertex w and that the edge between v_1 and w is in M. This edge cannot be in N, for then there would be two edges of N incident at v_1. But then this edge is in G', since it is in M but not N, and therefore the path in G' does not start with the edge in N joining v_1 and v_2. This contradiction shows that no edge of M is incident at v_1. The proof that the last vertex in the path is likewise not incident with an edge of M is essentially identical. ■

Now to find a maximum matching, we repeatedly look for alternating chains; when we cannot find one, we know we have a maximum matching. What we need now is an efficient algorithm for finding the alternating chain.

The key, in a sense, is to look for all possible alternating chains simultaneously. Suppose we have a bipartite graph with vertex partition $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_m\}$ and a matching M. The algorithm labels vertices in such a way that if it succeeds, the alternating chain is indicated by the labels. Here are the steps:

0. Label with '(S,0)' all vertices v_i that are not incident with an edge in M. Set variable *step* to 0.

Now repeat the next two steps until no vertex acquires a new label:

1. Increase *step* by 1. For each newly labeled vertex v_i, label with $(i, step)$ any unlabeled neighbor w_j of v_i that is connected to v_i by an edge that is not in M.

2. Increase *step* by 1. For each newly labeled vertex w_i, label with $(i, step)$ any unlabeled neighbor v_j of w_i that is connected to w_i by an edge in M.

Here "newly labeled" means labeled at the previous step. When labeling vertices in step 1 or 2, no vertex is given more than one label. For example, in step 1, it may be that w_k is a neighbor of the newly labeled vertices v_i and v_j. One of v_i and v_j, say v_i, will be considered first, and will cause w_k to be labeled; when v_j is considered, w_k is no longer unlabeled.

At the conclusion of the algorithm, if there is a labeled vertex w_i that is not incident with any edge of M, then there is an alternating chain, and we say the algorithm succeeds. If there is no such w_i, then there is no alternating chain, and we say the algorithm fails. The first of these claims is easy to see: Suppose vertex w_i is labeled (k_1, s). It became labeled due to vertex v_{k_1} labeled $(k_2, s-1)$ that is connected by an edge not in M to w_i. In turn, v_{k_1} is connected by an edge in M to vertex w_{k_2} labeled $(k_3, s-2)$. Continuing in this way, we discover an alternating chain ending at some vertex v_j labeled $(S, 0)$: since the second coordinate *step* decreases by 1 at each vertex along the chain, we cannot repeat vertices, and must eventually get to a vertex with $step = 0$. If we apply the algorithm to the graph in figure 4.5.2, we get the labeling shown in figure 4.5.5, which then identifies the alternating chain w_2, v_3, w_1, v_1. Note that as soon as a vertex w_i that is incident with no edge of M is labeled, we may stop, as there must be an alternating chain starting at w_i; we need not continue the algorithm until no more labeling is possible. In the example in figure 4.5.5, we could stop after step 3, when w_2 becomes labeled. Also, the *step* component of the labels is not really needed; it was included to make it easier to understand that if the algorithm succeeds, there really is an alternating chain.

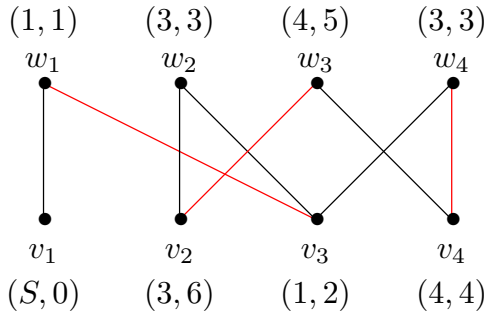


Figure 4.5.5 Labeling of a bipartite graph with matching; w_2, v_3, w_1, v_1 is an alternating chain.

To see that when the algorithm fails there is no alternating chain, we introduce a new concept.

DEFINITION 4.5.3 A **vertex cover** in a graph is a set of vertices S such that every edge in the graph has at least one endpoint in S. □

There is always a vertex cover of a graph, namely, the set of all the vertices of the graph. What is clearly more interesting is a smallest vertex cover, which is related to a maximum matching.

THEOREM 4.5.4 If M is a matching in a graph and S is a vertex cover, then $|M| \leq |S|$.

Proof. Suppose M is a matching S is a vertex cover. Since each edge of M has an endpoint in S, if $|M| > |S|$ then some vertex in S is incident with two edges of M, a contradiction. Hence $|M| \leq |S|$. ■

Suppose that we have a matching M and vertex cover S for a graph, and that $|M| = |S|$. Then the theorem implies that M is a maximum matching and S is a minimum vertex cover. To show that when the algorithm fails there is no alternating chain, it is sufficient to show that there is a vertex cover that is the same size as M. Note that the proof of this theorem relies on the "official" version of the algorithm, that is, the algorithm continues until no new vertices are labeled.

THEOREM 4.5.5 Suppose the algorithm fails on the bipartite graph G with matching M. Let L be the set of labeled w_i, U the set of unlabeled v_i, and $S = L \cup U$. Then S is a vertex cover and $|M| = |S|$.

Proof. If S is not a cover, there is an edge $\{v_i, w_j\}$ with neither v_i nor w_j in S, so v_i is labeled and w_j is not. If the edge is not in M, then the algorithm would have labeled w_j at the step after v_i became labeled, so the edge must be in M. Now v_i cannot be labeled $(S, 0)$, so v_i became labeled because it is connected to some labeled w_k by an edge of M. But now the two edges $\{v_i, w_j\}$ and $\{v_i, w_k\}$ are in M, a contradiction. So S is a vertex cover.

We know that $|M| \leq |S|$, so it suffices to show $|S| \leq |M|$, which we can do by finding an injection from S to M. Suppose that $w_i \in S$, so w_i is labeled. Since the algorithm failed, w_i is incident with an edge e of M; let $f(w_i) = e$. If $v_i \in S$, v_i is unlabeled; if v_i were not incident with any edge of M, then v_i would be labeled $(S, 0)$, so v_i is incident with an edge e of M; let $f(v_i) = e$. Since G is bipartite, it is not possible that $f(w_i) = f(w_j)$ or $f(v_i) = f(v_j)$. If $f(w_i) = f(v_j)$, then w_i and v_j are joined by an edge of M, and the algorithm would have labeled v_j. Hence, f is an injection. ■

We have now proved this theorem:

THEOREM 4.5.6 In a bipartite graph G, the size of a maximum matching is the same as the size of a minimum vertex cover. ■

It is clear that the size of a maximum SDR is the same as the size of a maximum matching in the associated bipartite graph G. It is not too difficult to see directly that the size of a minimum vertex cover in G is the minimum value of $f(n, i_1, i_2, \ldots, i_k) = n - k + |\bigcup_{j=1}^{k} A_{i_j}|$. Thus, if the size of a maximum matching is equal to the size of a minimum cover, then the size of a maximum SDR is equal to the minimum value of $n - k + |\bigcup_{j=1}^{k} A_{i_j}|$, and conversely. More concisely, theorem 4.5.6 is true if and only if theorem 4.2.1 is true.

More generally, in the schematic of figure 4.5.6, if any three of the relationships are known to be true, so is the fourth. In fact, we have proved all but the bottom equality, so we know it is true as well.

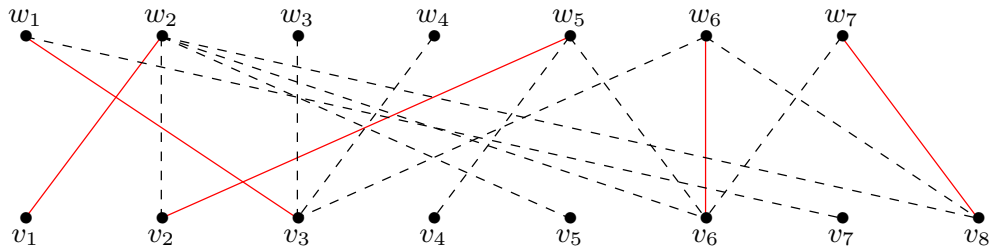
$$\begin{array}{ccc} \text{max sdr} & =? & \text{max matching} \\ \| ? & & \| ? \\ \text{min } f(n, \ldots) & =? & \text{min cover} \end{array}$$

Figure 4.5.6 If any three of the "=?" are "=", so is the fourth.

Finally, note that we now have both a more efficient way to compute the size of a maximum SDR and a way to find the actual representatives: convert the SDR problem to the graph problem, find a maximum matching, and interpret the matching as an SDR.

Exercises 4.5.

1. In this bipartite graph, find a maximum matching and a minimum vertex cover using the algorithm of this section. Start with the matching shown in red. Copies of this graph are available in this pdf file.



2. Show directly that that the size of a minimum vertex cover in G is the minimum value of $n - k + |\bigcup_{j=1}^{k} A_{i_j}|$, as mentioned above.

5

Graph Theory

5.1 The Basics

See section 4.4 to review some basic terminology about graphs.

A graph G consists of a pair (V, E), where V is the set of vertices and E the set of edges. We write $V(G)$ for the vertices of G and $E(G)$ for the edges of G when necessary to avoid ambiguity, as when more than one graph is under discussion.

If no two edges have the same endpoints we say there are no **multiple edges**, and if no edge has a single vertex as both endpoints we say there are no **loops**. A graph with no loops and no multiple edges is a **simple graph**. A graph with no loops, but possibly with multiple edges is a **multigraph**. The **condensation** of a multigraph is the simple graph formed by eliminating multiple edges, that is, removing all but one of the edges with the same endpoints. To form the condensation of a graph, all loops are also removed. We sometimes refer to a graph as a **general graph** to emphasize that the graph may have loops or multiple edges.

The edges of a simple graph can be represented as a set of two element sets; for example,

$$(\{v_1, \ldots, v_7\}, \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_7\}\})$$

is a graph that can be pictured as in figure 5.1.1. This graph is also a **connected** graph: each pair of vertices v, w is connected by a sequence of vertices and edges, $v = v_1, e_1, v_2, e_2, \ldots, v_k = w$, where v_i and v_{i+1} are the endpoints of edge e_i. The graphs shown in figure 4.4.2 are connected, but the figure could be interpreted as a single graph that is not connected.

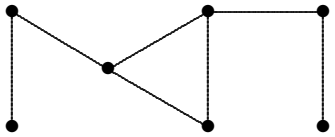


Figure 5.1.1 A simple graph.

A graph $G = (V, E)$ that is not simple can be represented by using multisets: a loop is a multiset $\{v, v\} = \{2 \cdot v\}$ and multiple edges are represented by making E a multiset. The condensation of a multigraph may be formed by interpreting the multiset E as a set.

A general graph that is not connected, has loops, and has multiple edges is shown in figure 5.1.2. The condensation of this graph is shown in figure 5.1.3.

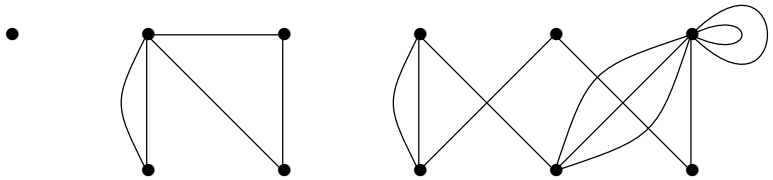


Figure 5.1.2 A general graph: it is not connected and has loops and mulitple edges.

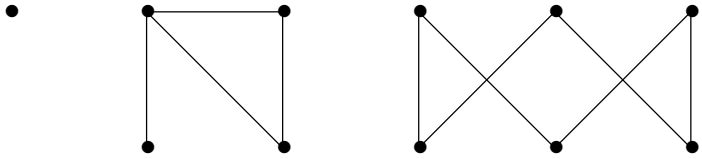


Figure 5.1.3 The condensation of the previous graph.

The degree of a a vertex v, $\mathrm{d}(v)$, is the number of times it appears as an endpoint of an edge. If there are no loops, this is the same as the number of edges incident with v, but if v is both endpoints of an edge, namely, of a loop, then this contributes 2 to the degree of v. The **degree sequence** of a graph is a list of its degrees; the order does not matter, but usually we list the degrees in increasing or decreasing order. The degree sequence of the graph in figure 5.1.2, listed clockwise starting at the upper left, is $0, 4, 2, 3, 2, 8, 2, 4, 3, 2, 2$. We typically denote the degrees of the vertices of a graph by d_i, $i = 1, 2, \ldots, n$, where n is the number of vertices. Depending on context, the subscript i may match the subscript on a vertex, so that d_i is the degree of v_i, or the subscript may indicate the position of d_i in an increasing or decreasing list of the degrees; for example, we may state that the degree sequence is $d_1 \leq d_2 \leq \cdots \leq d_n$.

Our first result, simple but useful, concerns the degree sequence.

THEOREM 5.1.1 In any graph, the sum of the degree sequence is equal to twice the number of edges, that is,

$$\sum_{i=1}^{n} d_i = 2|E|.$$

Proof. Let d_i be the degree of v_i. The degree d_i counts the number of times v_i appears as an endpoint of an edge. Since each edge has two endpoints, the sum $\sum_{i=1}^{n} d_i$ counts each edge twice. ■

An easy consequence of this theorem:

COROLLARY 5.1.2 The number of odd numbers in a degree sequence is even. ■

An interesting question immediately arises: given a finite sequence of integers, is it the degree sequence of a graph? Clearly, if the sum of the sequence is odd, the answer is no. If the sum is even, it is not too hard to see that the answer is yes, provided we allow loops and multiple edges. The sequence need not be the degree sequence of a simple graph; for example, it is not hard to see that no simple graph has degree sequence $0, 1, 2, 3, 4$. A sequence that is the degree sequence of a simple graph is said to be **graphical**. Graphical sequences have been characterized; the most well known characterization is given by this result:

THEOREM 5.1.3 A sequence $d_1 \geq d_2 \geq \ldots \geq d_n$ is graphical if and only if $\sum_{i=1}^{n} d_i$ is even and for all $k \in \{1, 2, \ldots, n\}$,

$$\sum_{i=1}^{k} d_i \leq k(k-1) + \sum_{i=k+1}^{n} \min(d_i, k).$$

■

It is not hard to see that if a sequence is graphical it has the property in the theorem; it is rather more difficult to see that any sequence with the property is graphical.

What does it mean for two graphs to be the same? Consider these three graphs:

$$G_1 = (\{v_1, v_2, v_3, v_4\}, \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_2, v_4\}\})$$
$$G_2 = (\{v_1, v_2, v_3, v_4\}, \{\{v_1, v_2\}, \{v_1, v_4\}, \{v_3, v_4\}, \{v_2, v_4\}\})$$
$$G_3 = (\{w_1, w_2, w_3, w_4\}, \{\{w_1, w_2\}, \{w_1, w_4\}, \{w_3, w_4\}, \{w_2, w_4\}\})$$

These are pictured in figure 5.1.4. Simply looking at the lists of vertices and edges, they don't appear to be the same. Looking more closely, G_2 and G_3 are the same except for the names used for the vertices: v_i in one case, w_i in the other. Looking at the pictures, there is an obvious sense in which all three are the same: each is a triangle with an edge

(and vertex) dangling from one of the three vertices. Although G_1 and G_2 use the same names for the vertices, they apply to different vertices in the graph: in G_1 the "dangling" vertex (officially called a **pendant** vertex) is called v_1, while in G_2 it is called v_3. Finally, note that in the figure, G_2 and G_3 look different, even though they are clearly the same based on the vertex and edge lists.

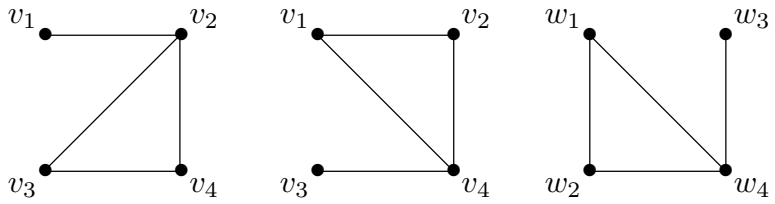


Figure 5.1.4 Three isomorphic graphs.

So how should we define "sameness" for graphs? We use a familiar term and definition: isomorphism.

DEFINITION 5.1.4 Suppose $G_1 = (V, E)$ and $G_2 = (W, F)$. G_1 and G_2 are **isomorphic** if there is a bijection $f: V \to W$ such that $\{v_1, v_2\} \in E$ if and only if $\{f(v_1), f(v_2)\} \in F$. In addition, the repetition numbers of $\{v_1, v_2\}$ and $\{f(v_1), f(v_2)\}$ are the same if multiple edges or loops are allowed. This bijection f is called an **isomorphism**. When G_1 and G_2 are isomorphic, we write $G_1 \cong G_2$. □

Each pair of graphs in figure 5.1.4 are isomorphic. For example, to show explicitly that $G_1 \cong G_3$, an isomorphism is

$$f(v_1) = w_3$$
$$f(v_2) = w_4$$
$$f(v_3) = w_2$$
$$f(v_4) = w_1.$$

Clearly, if two graphs are isomorphic, their degree sequences are the same. The converse is not true; the graphs in figure 5.1.5 both have degree sequence $1, 1, 1, 2, 2, 3$, but in one the degree-2 vertices are adjacent to each other, while in the other they are not. In general, if two graphs are isomorphic, they share all "graph theoretic" properties, that is, properties that depend only on the graph. As an example of a non-graph theoretic property, consider "the number of times edges cross when the graph is drawn in the plane."

In a more or less obvious way, some graphs are contained in others.

DEFINITION 5.1.5 Graph $H = (W, F)$ is a **subgraph** of graph $G = (V, E)$ if $W \subseteq V$ and $F \subseteq E$. (Since H is a graph, the edges in F have their endpoints in W.) H is an

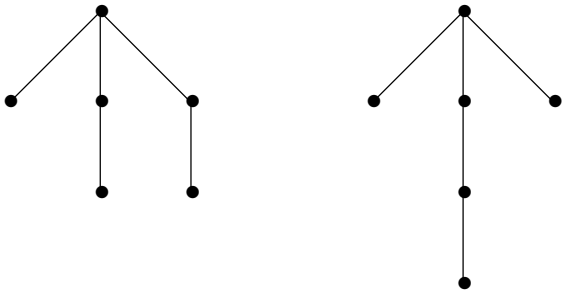


Figure 5.1.5 Non-isomorphic graphs with degree sequence $1, 1, 1, 2, 2, 3$.

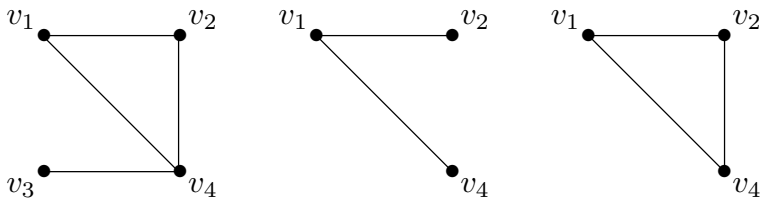


Figure 5.1.6 Left to right: a graph, a subgraph, an induced subgraph.

induced subgraph if F consists of all edges in E with endpoints in W. See figure 5.1.6. Whenever $U \subseteq V$ we denote the induced subgraph of G on vertices U as $G[U]$. □

A path in a graph is a subgraph that is a path; if the endpoints of the path are v and w we say it is a path from v to w. A cycle in a graph is a subgraph that is a cycle. A **clique** in a graph is a subgraph that is a complete graph.

If a graph G is not connected, define $v \sim w$ if and only if there is a path connecting v and w. It is not hard to see that this is an equivalence relation. Each equivalence class corresponds to an induced subgraph G; these subgraphs are called the **connected components** of the graph.

Exercises 5.1.

1. The complement $\overline{G}$ of the simple graph G is a simple graph with the same vertices as G, and $\{v, w\}$ is an edge of $\overline{G}$ if and only if it is not an edge of G. A graph G is self-complementary if $G \cong \overline{G}$. Show that if G is self-complementary then it has $4k$ or $4k + 1$ vertices for some k. Find self-complementary graphs on 4 and 5 vertices.
2. Prove that if $\sum_{i=1}^{n} d_i$ is even, there is a graph (not necessarily simple) with degree sequence $d_1, d_2, \ldots, d_n$.
3. Suppose $d_1 \geq d_2 \geq \cdots \geq d_n$ and $\sum_{i=1}^{n} d_i$ is even. Prove that there is a multigraph (no loops) with degree sequence $d_1, d_2, \ldots, d_n$ if and only if $d_1 \leq \sum_{i=2}^{n} d_i$.
4. Prove that $0, 1, 2, 3, 4$ is not graphical.
5. Is $4, 4, 3, 2, 2, 1, 1$ graphical? If not, explain why; if so, find a simple graph with this degree sequence.

6. Is $4, 4, 4, 2, 2$ graphical? If not, explain why, and find a multigraph (no loops) with this degree sequence; if so, find a simple graph with this degree sequence.
7. Prove that a simple graph with $n \geq 2$ vertices has two vertices of the same degree.
8. Prove the "only if" part of theorem 5.1.3.
9. Show that the condition on the degrees in theorem 5.1.3 is equivalent to this condition: $\sum_{i=1}^{n} d_i$ is even and for all $k \in \{1, 2, \ldots, n\}$, and all $\{i_1, i_2, \ldots, i_k\} \subseteq [n]$,

$$\sum_{j=1}^{k} d_{i_j} \leq k(k-1) + \sum_{i \notin \{i_1, i_2, \ldots, i_k\}} \min(d_i, k).$$

   Do not use theorem 5.1.3.
10. Draw the 11 non-isomorphic graphs with four vertices.
11. Suppose $G_1 \cong G_2$. Show that if G_1 contains a cycle of length k so does G_2.
12. Define $v \sim w$ if and only if there is a path connecting vertices v and w. Prove that $\sim$ is an equivalence relation.
13. Prove the "if" part of theorem 5.1.3, as follows:

    The proof is by induction on $s = \sum_{i=1}^{n} d_i$. This is easy to see if $s = 2$, so suppose $s > 2$. Without loss of generality we may suppose that $d_n > 0$. Let t be the least integer such that $d_t > d_{t+1}$, or $t = n - 1$ if there is no such integer. Let $d'_t = d_t - 1$, $d'_n = d_n - 1$, and $d'_i = d_i$ for all other i. Note that $d'_1 \geq d'_2 \geq \cdots d'_n$. We want to show that the sequence $\{d'_i\}$ satisfies the condition of the theorem, that is, that for all $k \in \{1, 2, \ldots, n\}$,

$$\sum_{i=1}^{k} d'_i \leq k(k-1) + \sum_{i=k+1}^{n} \min(d'_i, k).$$

    There are five cases:

    1. $k \geq t$
    2. $k < t$, $d_k < k$
    3. $k < t$, $d_k = k$
    4. $k < t$, $d_n > k$
    5. $k < t$, $d_k > k$, $d_n \leq k$

    By the induction hypothesis, there is a simple graph with degree sequence $\{d'_i\}$. Finally, show that there is a graph with degree sequence $\{d_i\}$.

    This proof is due to S. A. Choudum, *A Simple Proof of the Erdős-Gallai Theorem on Graph Sequences*, Bulletin of the Australian Mathematics Society, vol. 33, 1986, pp. 67-70. The proof by Paul Erdős and Tibor Gallai was long; Berge provided a shorter proof that used results in the theory of network flows. Choudum's proof is both short and elementary.

5.2 Euler Circuits and Walks

The first problem in graph theory dates to 1735, and is called the Seven Bridges of Königsberg. In Königsberg were two islands, connected to each other and the mainland by seven bridges, as shown in figure 5.2.1. The question, which made its way to Euler,

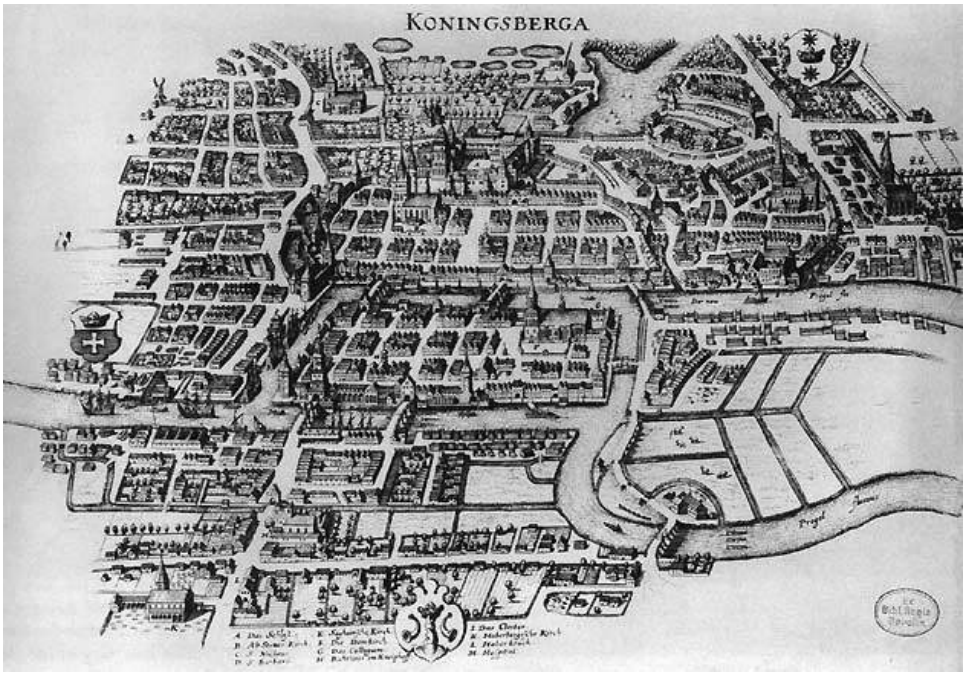


Figure 5.2.1 The Seven Bridges of Königsberg.

was whether it was possible to take a walk and cross over each bridge exactly once; Euler showed that it is not possible.

We can represent this problem as a graph, as in figure 5.2.2.

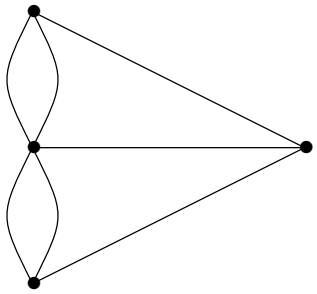


Figure 5.2.2 The Seven Bridges of Königsberg as a graph.

The two sides of the river are represented by the top and bottom vertices, and the islands by the middle two vertices. There are two possible interpretations of the question, depending on whether the goal is to end the walk at its starting point. Perhaps inspired by this problem, a **walk** in a graph is defined as follows.

DEFINITION 5.2.1 A walk in a graph is a sequence of vertices and edges,

$$v_1, e_1, v_2, e_2, \ldots, v_k, e_k, v_{k+1}$$

such that the endpoints of edge e_i are v_i and v_{i+1}. In general, the edges and vertices may appear in the sequence more than once. If $v_1 = v_{k+1}$, the walk is a **closed walk** or a **circuit**. □

We will deal first with the case in which the walk is to start and end at the same place. A successful walk in Königsberg corresponds to a closed walk in the graph in which every edge is used exactly once.

What can we say about this walk in the graph, or indeed a closed walk in any graph that uses every edge exactly once? Such a walk is called an **Euler circuit**. If there are no vertices of degree 0, the graph must be connected, as this one is. Beyond that, imagine tracing out the vertices and edges of the walk on the graph. At every vertex other than the common starting and ending point, we come into the vertex along one edge and go out along another; this can happen more than once, but since we cannot use edges more than once, the number of edges incident at such a vertex must be even. Already we see that we're in trouble in this particular graph, but let's continue the analysis. The common starting and ending point may be visited more than once; except for the very first time we leave the starting vertex, and the last time we arrive at the vertex, each such visit uses exactly two edges. Together with the edges used first and last, this means that the starting vertex must also have even degree. Thus, since the Königsberg Bridges graph has odd degrees, the desired walk does not exist.

The question that should immediately spring to mind is this: if a graph is connected and the degree of every vertex is even, is there an Euler circuit? The answer is yes.

THEOREM 5.2.2 If G is a connected graph, then G contains an Euler circuit if and only if every vertex has even degree.

Proof. We have already shown that if there is an Euler circuit, all degrees are even.

We prove the other direction by induction on the number of edges. If G has no edges the problem is trivial, so we assume that G has edges.

We start by finding some closed walk that does not use any edge more than once: Start at any vertex v_0; follow any edge from this vertex, and continue to do this at each new vertex, that is, upon reaching a vertex, choose some unused edge leading to another vertex. Since every vertex has even degree, it is always possible to leave a vertex at which we arrive, until we return to the starting vertex, and every edge incident with the starting vertex has been used. The sequence of vertices and edges formed in this way is a closed walk; if it uses every edge, we are done.

Otherwise, form graph G' by removing all the edges of the walk. G' is not connected, since vertex v_0 is not incident with any remaining edge. The rest of the graph, that is, G' without v_0, may or may not be connected. It consists of one or more connected subgraphs, each with fewer edges than G; call these graphs G_1, G_2,...,G_k. Note that when we remove

the edges of the initial walk, we reduce the degree of every vertex by an even number, so all the vertices of each graph G_i have even degree. By the induction hypothesis, each G_i has an Euler circuit. These closed walks together with the original closed walk use every edge of G exactly once.

Suppose the original closed walk is $v_0, v_1, \ldots, v_m = v_0$, abbreviated to leave out the edges. Because G is connected, at least one vertex in each G_i appears in this sequence, say vertices $w_{1,1} \in G_1$, $w_{2,1} \in G_2, \ldots$, $w_{k,1} \in G_k$, listed in the order they appear in $v_0, v_1, \ldots, v_m$. The Euler circuits of the graphs G_i are

$$\begin{aligned} &w_{1,1}, w_{1,2}, \ldots, w_{1,m_1} = w_{1,1} \\ &w_{2,1}, w_{2,2}, \ldots, w_{2,m_2} = w_{2,1} \\ &\vdots \\ &w_{k,1}, w_{k,2}, \ldots, w_{k,m_k} = w_{k,1}. \end{aligned}$$

By pasting together the original closed walk with these, we form a closed walk in G that uses every edge exactly once:

$$\begin{aligned} v_0, v_1, \ldots, v_{i_1} = w_{1,1}, w_{1,2}, \ldots, w_{1,m_1} = v_{i_1}, v_{i_1+1}, \\ \ldots, v_{i_2} = w_{2,1}, \ldots, w_{2,m_2} = v_{i_2}, v_{i_2+1}, \\ \ldots, v_{i_k} = w_{k,1}, \ldots, w_{k,m_k} = v_{i_k}, v_{i_k+1}, \ldots, v_m = v_0. \end{aligned}$$

■

Now let's turn to the second interpretation of the problem: is it possible to walk over all the bridges exactly once, if the starting and ending points need not be the same? In a graph G, a walk that uses all of the edges but is not an Euler circuit is called an **Euler walk**. It is not too difficult to do an analysis much like the one for Euler circuits, but it is even easier to use the Euler circuit result itself to characterize Euler walks.

THEOREM 5.2.3 A connected graph G has an Euler walk if and only if exactly two vertices have odd degree.

Proof. Suppose first that G has an Euler walk starting at vertex v and ending at vertex w. Add a new edge to the graph with endpoints v and w, forming G'. G' has an Euler circuit, and so by the previous theorem every vertex has even degree. The degrees of v and w in G are therefore odd, while all others are even.

Now suppose that the degrees of v and w in G are odd, while all other vertices have even degree. Add a new edge e to the graph with endpoints v and w, forming G'. Every vertex in G' has even degree, so by the previous theorem there is an Euler circuit which

we can write as

$$v, e_1, v_2, e_2, \ldots, w, e, v$$

so that

$$v, e_1, v_2, e_2, \ldots, w$$

is an Euler walk. ■

Exercises 5.2.

1. Suppose a connected graph G has degree sequence $d_1, d_2, \ldots, d_n$. How many edges must be added to G so that the resulting graph has an Euler circuit? Explain.
2. Which complete graphs K_n, $n \geq 2$, have Euler circuits? Which have Euler walks? Justify your answers.
3. Prove that if vertices v and w are joined by a walk they are joined by a path.
4. Show that if G is connected and has exactly $2k$ vertices of odd degree, $k \geq 1$, its edges can be partitioned into k walks. Is this true for non-connected G?

5.3 Hamilton Cycles and Paths

Here is a problem similar to the Königsberg Bridges problem: suppose a number of cities are connected by a network of roads. Is it possible to visit all the cities exactly once, without traveling any road twice? We assume that these roads do not intersect except at the cities. Again there are two versions of this problem, depending on whether we want to end at the same city in which we started.

This problem can be represented by a graph: the vertices represent cities, the edges represent the roads. We want to know if this graph has a cycle, or path, that uses every vertex exactly once. (Recall that a cycle in a graph is a subgraph that is a cycle, and a path is a subgraph that is a path.) There is no benefit or drawback to loops and multiple edges in this context: loops can never be used in a Hamilton cycle or path (except in the trivial case of a graph with a single vertex), and at most one of the edges between two vertices can be used. So we assume for this discussion that all graphs are simple.

DEFINITION 5.3.1 A cycle that uses every vertex in a graph exactly once is called a **Hamilton cycle**, and a path that uses every vertex in a graph exactly once is called a **Hamilton path**. □

Unfortunately, this problem is much more difficult than the corresponding Euler circuit and walk problems; there is no good characterization of graphs with Hamilton paths and cycles. Note that if a graph has a Hamilton cycle then it also has a Hamilton path.

There are some useful conditions that imply the existence of a Hamilton cycle or path, which typically say in some form that there are many edges in the graph. An extreme

example is the complete graph K_n: it has as many edges as any simple graph on n vertices can have, and it has many Hamilton cycles.

The problem for a characterization is that there are graphs with Hamilton cycles that do not have very many edges. The simplest is a cycle, C_n: this has only n edges but has a Hamilton cycle. On the other hand, figure 5.3.1 shows graphs with just a few more edges than the cycle on the same number of vertices, but without Hamilton cycles.

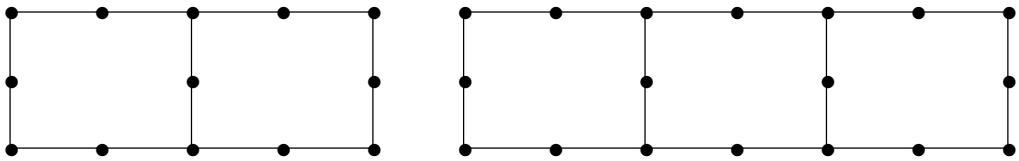


Figure 5.3.1 A graph with a Hamilton path but not a Hamilton cycle, and one with neither.

There are also graphs that seem to have many edges, yet have no Hamilton cycle, as indicated in figure 5.3.2.

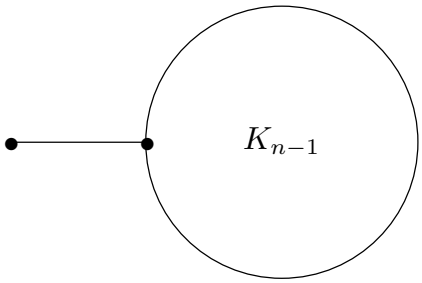


Figure 5.3.2 A graph with many edges but no Hamilton cycle: a complete graph K_{n-1} joined by an edge to a single vertex. This graph has $\binom{n-1}{2} + 1$ edges.

The key to a successful condition sufficient to guarantee the existence of a Hamilton cycle is to require many edges at lots of vertices.

THEOREM 5.3.2 (Ore) If G is a simple graph on n vertices, $n \geq 3$, and $\mathrm{d}(v) + \mathrm{d}(w) \geq n$ whenever v and w are not adjacent, then G has a Hamilton cycle.

Proof. First we show that G is connected. If not, let v and w be vertices in two different connected components of G, and suppose the components have n_1 and n_2 vertices. Then $\mathrm{d}(v) \leq n_1 - 1$ and $\mathrm{d}(w) \leq n_2 - 1$, so $\mathrm{d}(v) + \mathrm{d}(w) \leq n_1 + n_2 - 2 < n$. But since v and w are not adjacent, this is a contradiction.

Now consider a longest possible path in G: $v_1, v_2, \ldots, v_k$. Suppose, for a contradiction, that $k < n$, so there is some vertex w adjacent to one of $v_2, v_3, \ldots, v_{k-1}$, say to v_i. If v_1 is adjacent to v_k, then $w, v_i, v_{i+1}, \ldots, v_k, v_1, v_2, \ldots v_{i-1}$ is a path of length $k+1$, a contradiction. Hence, v_1 is not adjacent to v_k, and so $\mathrm{d}(v_1) + d(v_k) \geq n$. The neighbors of

v_1 are among $\{v_2, v_3, \ldots, v_{k-1}\}$ as are the neighbors of v_k. Consider the vertices

$$W = \{v_{l+1} \mid v_l \text{ is a neighbor of } v_k\}.$$

Then $|N(v_k)| = |W|$ and $W \subseteq \{v_3, v_4, \ldots, v_k\}$ and $N(v_1) \subseteq \{v_2, v_3, \ldots, v_{k-1}\}$, so $W \cup N(v_1) \subseteq \{v_2, v_3, \ldots, v_k\}$, a set with $k-1 < n$ elements. Since $|N(v_1)| + |W| = |N(v_1)| + |N(v_k)| \geq n$, $N(v_1)$ and W must have a common element, v_j; note that $3 \leq j \leq k-1$. Then this is a cycle of length k:

$$v_1, v_j, v_{j+1}, \ldots, v_k, v_{j-1}, v_{j-2}, \ldots, v_1.$$

We can relabel the vertices for convenience:

$$v_1 = w_1, w_2, \ldots, w_k = v_2, w_1.$$

Now as before, w is adjacent to some w_l, and $w, w_l, w_{l+1}, \ldots, w_k, w_1, w_2, \ldots w_{l-1}$ is a path of length $k+1$, a contradiction. Thus, $k = n$, and, renumbering the vertices for convenience, we have a Hamilton path $v_1, v_2, \ldots, v_n$. If v_1 is adjacent to v_n, there is a Hamilton cycle, as desired.

If v_1 is not adjacent to v_n, the neighbors of v_1 are among $\{v_2, v_3, \ldots, v_{n-1}\}$ as are the neighbors of v_n. Consider the vertices

$$W = \{v_{l+1} \mid v_l \text{ is a neighbor of } v_n\}.$$

Then $|N(v_n)| = |W|$ and $W \subseteq \{v_3, v_4, \ldots, v_n\}$, and $N(v_1) \subseteq \{v_2, v_3, \ldots, v_{n-1}\}$, so $W \cup N(v_1) \subseteq \{v_2, v_3, \ldots, v_n\}$, a set with $n-1 < n$ elements. Since $|N(v_1)| + |W| = |N(v_1)| + |N(v_n)| \geq n$, $N(v_1)$ and W must have a common element, v_i; note that $3 \leq i \leq n-1$. Then this is a cycle of length n:

$$v_1, v_i, v_{i+1}, \ldots, v_k, v_{i-1}, v_{i-2}, \ldots, v_1,$$

and is a Hamilton cycle. ■

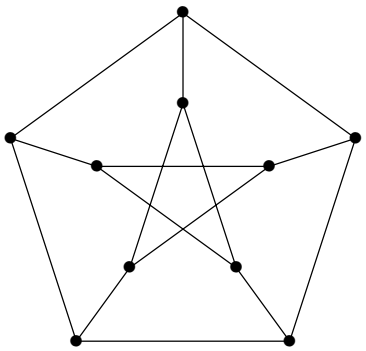
The property used in this theorem is called the **Ore property**; if a graph has the Ore property it also has a Hamilton path, but we can weaken the condition slightly if our goal is to show there is a Hamilton path. The proof of this theorem is nearly identical to the preceding proof.

THEOREM 5.3.3 If G is a simple graph on n vertices and $\mathrm{d}(v)+\mathrm{d}(w) \geq n-1$ whenever v and w are not adjacent, then G has a Hamilton path. ■

Suppose G is not simple. The existence of multiple edges and loops can't help produce a Hamilton cycle when $n \geq 3$: if we use a second edge between two vertices, or use a loop, we have repeated a vertex. To extend the Ore theorem to multigraphs, we consider the condensation of G: When $n \geq 3$, the condensation of G is simple, and has a Hamilton cycle if and only if G has a Hamilton cycle. So if the condensation of G satisfies the Ore property, then G has a Hamilton cycle.

Exercises 5.3.

1. Suppose a simple graph G on n vertices has at least $\frac{(n-1)(n-2)}{2}+2$ edges. Prove that G has a Hamilton cycle. For $n \geq 2$, show that there is a simple graph with $\frac{(n-1)(n-2)}{2}+1$ edges that has no Hamilton cycle.
2. Prove theorem 5.3.3.
3. The graph shown below is the **Petersen** graph. Does it have a Hamilton cycle? Justify your answer. Does it have a Hamilton path? Justify your answer.



5.4 Bipartite Graphs

We have already seen how bipartite graphs arise naturally in some circumstances. Here we explore bipartite graphs a bit more.

It is easy to see that all closed walks in a bipartite graph must have even length, since the vertices along the walk must alternate between the two parts. Remarkably, the converse is true. We need one new definition:

DEFINITION 5.4.1 The distance between vertices v and w, $\mathrm{d}(v,w)$, is the length of a shortest walk between the two. If there is no walk between v and w, the distance is undefined. □

THEOREM 5.4.2 G is bipartite if and only if all closed walks in G are of even length.

Proof. The forward direction is easy, as discussed above.

Now suppose that all closed walks have even length. We may assume that G is connected; if not, we deal with each connected component separately.

Let v be a vertex of G, let X be the set of all vertices at even distance from v, and Y be the set of vertices at odd distance from v. We claim that all edges of G join a vertex of X to a vertex of Y. Suppose not; then there are adjacent vertices u and w such that $\mathrm{d}(v,u)$ and $\mathrm{d}(v,w)$ have the same parity. Then there is a closed walk from v to u to w to v of length $\mathrm{d}(v,u)+1+\mathrm{d}(v,w)$, which is odd, a contradiction. ■

The closed walk that provides the contradiction is not necessarily a cycle, but this can be remedied, providing a slightly different version of the theorem.

COROLLARY 5.4.3 G is bipartite if and only if all cycles in G are of even length.

Proof. Again the forward direction is easy, and again we assume G is connected. As before, let v be a vertex of G, let X be the set of all vertices at even distance from v, and Y be the set of vertices at odd distance from v. If two vertices in X are adjacent, or two vertices in Y are adjacent, then as in the previous proof, there is a closed walk of odd length.

To finish the proof, it suffices to show that if there is a closed walk W of odd length then there is a cycle of odd length. The proof is by induction on the length of the closed walk.

If W has no repeated vertices, we are done. Otherwise, suppose the closed walk is

$$v = v_1, e_1, \ldots, v_i = v, \ldots, v_k = v = v_1.$$

Then

$$v = v_1, \ldots, v_i = v \quad \text{and} \quad v = v_i, e_i, v_{i+1}, \ldots, v_k = v$$

are closed walks, both are shorter than the original closed walk, and one of them has odd length. By the induction hypothesis, there is a cycle of odd length. ■

It is frequently fruitful to consider graph properties in the limited context of bipartite graphs (or other special types of graph). For example, what can we say about Hamilton cycles in simple bipartite graphs? Suppose the partition of the vertices of the bipartite graph is X and Y. Because any cycle alternates between vertices of the two parts of the bipartite graph, if there is a Hamilton cycle then $|X| = |Y| \geq 2$. In such a case, the degree of every vertex is at most $n/2$, where n is the number of vertices, namely $n = |X| + |Y|$. Thus the Ore condition ($\mathrm{d}(v) + \mathrm{d}(w) \geq n$ when v and w are not adjacent) is equivalent to $\mathrm{d}(v) = n/2$ for all v. This means the only simple bipartite graph that satisfies the Ore condition is the **complete bipartite graph** $K_{n/2,n/2}$, in which the two parts have size $n/2$ and every vertex of X is adjacent to every vertex of Y. The upshot is that the Ore property gives no interesting information about bipartite graphs.

Of course, as with more general graphs, there are bipartite graphs with few edges and a Hamilton cycle: any even length cycle is an example.

We note that, in general, a complete bipartite graph $K_{m,n}$ is a bipartite graph with $|X| = m$, $|Y| = n$, and every vertex of X is adjacent to every vertex of Y. The only such graphs with Hamilton cycles are those in which $m = n$.

Exercises 5.4.

1. Prove that there is a bipartite multigraph with degree sequence $d_1, \ldots, d_n$ if and only if there is a partition $\{I, J\}$ of $[n]$ such that
$$\sum_{i \in I} d_i = \sum_{i \in J} d_i.$$
2. What is the smallest number of edges that can be removed from K_5 to create a bipartite graph?
3. A **regular graph** is one in which the degree of every vertex is the same. Show that if G is a regular bipartite graph, and the common degree of the vertices is at least 1, then the two parts are the same size.
4. A **perfect matching** is one in which all vertices of the graph are incident with exactly one edge in the matching. Show that a regular bipartite graph with common degree at least 1 has a perfect matching. (We discussed matchings in section 4.5.)

5.5 Trees

Another useful special class of graphs:

DEFINITION 5.5.1 A connected graph G is a **tree** if it is **acyclic**, that is, it has no cycles. More generally, an acyclic graph is called a **forest**. □

Two small examples of trees are shown in figure 5.1.5. Note that the definition implies that no tree has a loop or multiple edges.

THEOREM 5.5.2 Every tree T is bipartite.

Proof. Since T has no cycles, it is true that every cycle of T has even length. By corollary 5.4.3, T is bipartite. ■

DEFINITION 5.5.3 A vertex of degree one is called a **pendant** vertex, and the edge incident to it is a pendant edge. □

THEOREM 5.5.4 Every tree on two or more vertices has at least one pendant vertex.

Proof. We prove the contrapositive. Suppose graph G has no pendant vertices. Starting at any vertex v, follow a sequence of distinct edges until a vertex repeats; this is possible because the degree of every vertex is at least two, so upon arriving at a vertex for the first time it is always possible to leave the vertex on another edge. When a vertex repeats for the first time, we have discovered a cycle. ■

This theorem often provides the key step in an induction proof, since removing a pendant vertex (and its pendant edge) leaves a smaller tree.

THEOREM 5.5.5 A tree on n vertices has exactly $n-1$ edges.

Proof. A tree on 1 vertex has 0 edges; this is the base case.

If T is a tree on $n \geq 2$ vertices, it has a pendant vertex. Remove this vertex and its pendant edge to get a tree T' on $n-1$ vertices. By the induction hypothesis, T' has $n-2$ edges; thus T has $n-1$ edges. ■

THEOREM 5.5.6 A tree with a vertex of degree $k \geq 1$ has at least k pendant vertices. In particular, every tree on at least two vertices has at least two pendant vertices.

Proof. The case $k = 1$ is obvious. Let T be a tree with n vertices, degree sequence $\{d_i\}_{i=1}^n$, and a vertex of degree $k \geq 2$, and let l be the number of pendant vertices. Without loss of generality, $1 = d_1 = d_2 = \cdots = d_l$ and $d_{l+1} = k$. Then

$$2(n-1) = \sum_{i=1}^{n} d_i = l + k + \sum_{i=l+2}^{n} d_i \geq l + k + 2(n-l-1).$$

This reduces to $l \geq k$, as desired.

If T is a tree on two vertices, each of the vertices has degree 1. If T has at least three vertices it must have a vertex of degree $k \geq 2$, since otherwise $2(n-1) = \sum_{i=1}^{n} d_i = n$, which implies $n = 2$. Hence it has at least $k \geq 2$ pendant vertices. ■

Trees are quite useful in their own right, but also for the study of general graphs.

DEFINITION 5.5.7 If G is a connected graph on n vertices, a **spanning tree** for G is a subgraph of G that is a tree on n vertices. □

THEOREM 5.5.8 Every connected graph has a spanning tree.

Proof. By induction on the number of edges. If G is connected and has zero edges, it is a single vertex, so G is already a tree.

Now suppose G has $m \geq 1$ edges. If G is a tree, it is its own spanning tree. Otherwise, G contains a cycle; remove one edge of this cycle. The resulting graph G' is still connected and has fewer edges, so it has a spanning tree; this is also a spanning tree for G. ■

In general, spanning trees are not unique, that is, a graph may have many spanning trees. It is possible for some edges to be in every spanning tree even if there are multiple spanning trees. For example, any pendant edge must be in every spanning tree, as must any edge whose removal disconnects the graph (such an edge is called a **bridge**.)

COROLLARY 5.5.9 If G is connected, it has at least $n-1$ edges; moreover, it has exactly $n-1$ edges if and only if it is a tree.

Proof. If G is connected, it has a spanning tree, which has $n-1$ edges, all of which are edges of G.

If G has $n-1$ edges, which must be the edges of its spanning tree, then G is a tree. ■

THEOREM 5.5.10 G is a tree if and only if there is a unique path between any two vertices.

Proof.

if: Since every two vertices are connected by a path, G is connected. For a contradiction, suppose there is a cycle in G; then any two vertices on the cycle are connected by at least two distinct paths, a contradiction.

only if: If G is a tree it is connected, so between any two vertices there is at least one path. For a contradiction, suppose there are two different paths from v to w:

$$v = v_1, v_2, \ldots, v_k = w \quad \text{and} \quad v = w_1, w_2, \ldots, w_l = w.$$

Let i be the smallest integer such that $v_i \neq w_i$. Then let j be the smallest integer greater than or equal to i such that $w_j = v_m$ for some m, which must be at least i. (Since $w_l = v_k$, such an m must exist.) Then $v_{i-1}, v_i, \ldots, v_m = w_j, w_{j-1}, \ldots, w_{i-1} = v_{i-1}$ is a cycle in G, a contradiction. See figure 5.5.1. ■

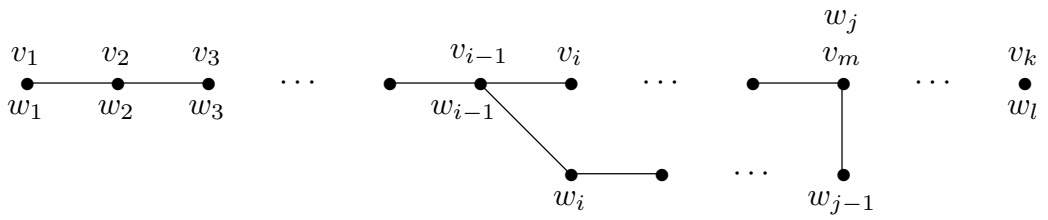


Figure 5.5.1 Distinct paths imply the existence of a cycle.

DEFINITION 5.5.11 A **cutpoint** in a connected graph G is a vertex whose removal disconnects the graph. □

THEOREM 5.5.12 Every connected graph has a vertex that is not a cutpoint.

Proof. Remove a pendant vertex in a spanning tree for the graph. ■

Exercises 5.5.

1. Suppose that G is a connected graph, and that every spanning tree contains edge e. Show that e is a bridge.
2. Show that every edge in a tree is a bridge.

3. Show that G is a tree if and only if it has no cycles and adding any new edge creates a graph with exactly one cycle.
4. Which trees have Euler walks?
5. Which trees have Hamilton paths?
6. Let $n \geq 2$. Show that there is a tree with degree sequence $d_1, d_2, \ldots, d_n$ if and only if $d_i > 0$ for all i and $\sum_{i=1}^{n} d_i = 2(n-1)$.
7. A multitree is a multigraph whose condensation is a tree. Let $n \geq 2$. Let $d_1, d_2, \ldots, d_n$ be positive integers, and let g be the greatest common divisor of the d_i. Show that there is a multitree with degree sequence $d_1, d_2, \ldots, d_n$ if and only if $\sum_{i=1}^{n} d_i/g \geq 2(n-1)$ and for some partition I, J of $[n]$, $\sum_{i \in I} d_i = \sum_{i \in J} d_i$.
8. Suppose T is a tree on n vertices, k of which have degree larger than 1, d_1, d_2,... d_k. Of course, T must also have pendant vertices. How many pendant vertices? Your answer should depend only on k and d_1, d_2,... d_k.

5.6 Optimal Spanning Trees

In some applications, a graph G is augmented by associating a weight or cost with each edge; such a graph is called a **weighted graph**. For example, if a graph represents a network of roads, the weight of an edge might be the length of the road between its two endpoints, or the amount of time required to travel from one endpoint to the other, or the cost to bury cable along the road from one end to the other. In such cases, instead of being interested in just any spanning tree, we may be interested in a **least cost spanning tree**, that is, a spanning tree such that the sum of the costs of the edges of the tree is as small as possible. For example, this would be the least expensive way to connect a set of towns by a communication network, burying the cable in such a way as to minimize the total cost of laying the cable.

This problem is one that can be solved by a **greedy algorithm**. Roughly speaking, a greedy algorithm is one that makes choices that are optimal in the short run. Typically this strategy does not result in an optimal solution in the long run, but in this case this approach works.

DEFINITION 5.6.1 A weighted graph is a graph G together with a cost function $c: E(G) \to \mathbb{R}^{>0}$. If H is a subgraph of G, the cost of H is $c(H) = \sum_{e \in E(H)} c(e)$. □

The Jarník Algorithm. Given a weighted connected graph G, we construct a minimum cost spanning tree T as follows. Choose any vertex v_0 in G and include it in T. If vertices $S = \{v_0, v_1, \ldots, v_k\}$ have been chosen, choose an edge with one endpoint in S and one endpoint not in S and with smallest weight among all such edges. Let v_{k+1} be the endpoint of this edge not in S, and add it and the associated edge to T. Continue until all vertices of G are in T.

This algorithm was discovered by Vojtěch Jarník in 1930, and rediscovered independently by Robert C. Prim in 1957 and Edsger Dijkstra in 1959. It is often called Prim's Algorithm.

The algorithm proceeds by constructing a sequence of trees $T_1, T_2, \ldots, T_{n-1}$, with T_{n-1} a spanning tree for G. At each step, the algorithm adds an edge that will make $c(T_{i+1})$ as small as possible among all trees that consist of T_i plus one edge. This is the best choice in the short run, but it is not obvious that in the long run, that is, by the time T_{n-1} is constructed, that this will turn out to have been the best choice.

THEOREM 5.6.2 The Jarník Algorithm produces a minimum cost spanning tree.

Proof. Suppose G is connected on n vertices. Let T be the spanning tree produced by the algorithm, and T_m a minimum cost spanning tree. We prove that $c(T) = c(T_m)$.

Let $e_1, e_2, \ldots, e_{n-1}$ be the edges of T in the order in which they were added to T; one endpoint of e_i is v_i, the other is in $\{v_0, \ldots, v_{i-1}\}$. We form a sequence of trees $T_m = T_0, T_1, \ldots, T_{n-1} = T$ such that for each i, $c(T_i) = c(T_{i+1})$, and we conclude that $c(T_m) = c(T)$.

If e_1 is in T_0, let $T_1 = T_0$. Otherwise, add edge e_1 to T_0. This creates a cycle containing e_1 and another edge incident at v_0, say f_1. Remove f_1 to form T_1. Since the algorithm added edge e_1, $c(e_1) \leq c(f_1)$. If $c(e_1) < c(f_1)$, then $c(T_1) < c(T_0) = c(T_m)$, a contradiction, so $c(e_1) = c(f_1)$ and $c(T_1) = c(T_0)$.

Suppose we have constructed tree T_i. If e_{i+1} is in T_i, let $T_{i+1} = T_i$. Otherwise, add edge e_{i+1} to T_i. This creates a cycle, one of whose edges, call it f_{i+1}, is not in $e_1, e_2, \ldots, e_i$ and has exactly one endpoint in $\{v_0, \ldots, v_i\}$. Remove f_{i+1} to create T_{i+1}. Since the algorithm added e_{i+1}, $c(e_{i+1}) \leq c(f_{i+1})$. If $c(e_{i+1}) < c(f_{i+1})$, then $c(T_{i+1}) < c(T_i) = c(T_m)$, a contradiction, so $c(e_{i+1}) = c(f_{i+1})$ and $c(T_{i+1}) = c(T_i)$. ■

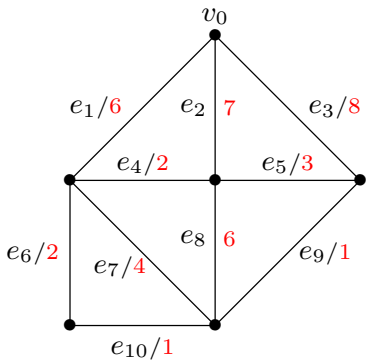
Exercises 5.6.

1. Kruskal's Algorithm is also a greedy algorithm that produces a minimum cost spanning tree for a connected graph G. Begin by choosing an edge in G of smallest cost. Assuming that edges $e_1, e_2, \ldots, e_i$ have been chosen, pick an edge e_{i+1} that does not form a cycle together with $e_1, e_2, \ldots, e_i$ and that has smallest cost among all such edges. The edges $e_1, e_2, \ldots, e_{n-1}$ form a spanning tree for G. Prove that this spanning tree has minimum cost.

2. Prove that if the edge costs of G are distinct, there is exactly one minimum cost spanning tree. Give an example of a graph G with more than one minimum cost spanning tree.

3. In both the Jarník and Kruskal algorithms, it may be that two or more edges can be added at any particular step, and some method is required to choose one over the other. For the graph below, use both algorithms to find a minimum cost spanning tree. Using the labels e_i on the graph, at each stage pick the edge e_i that the algorithm specifies and that has the lowest possible i among all edges available. For the Jarník algorithm, use the designated

v_0 as the starting vertex. For each algorithm, list the edges in the order in which they are added. The edge weights $e_1, e_2, \ldots, e_{10}$ are $6, 7, 8, 2, 3, 2, 4, 6, 1, 1$, shown in red.



5.7 Connectivity

We have seen examples of connected graphs and graphs that are not connected. While "not connected" is pretty much a dead end, there is much to be said about "how connected" a connected graph is. The simplest approach is to look at how hard it is to disconnect a graph by removing vertices or edges. We assume that all graphs are simple.

If it is possible to disconnect a graph by removing a single vertex, called a cutpoint, we say the graph has connectivity 1. If this is not possible, but it is possible to disconnect the graph by removing two vertices, the graph has connectivity 2.

DEFINITION 5.7.1 If a graph G is connected, any set of vertices whose removal disconnects the graph is called a **cutset**. G has connectivity k if there is a cutset of size k but no smaller cutset. If there is no cutset and G has at least two vertices, we say G has connectivity $n-1$; if G has one vertex, its connectivity is undefined. If G is not connected, we say it has connectivity 0. G is k-connected if the connectivity of G is at least k. The connectivity of G is denoted $\kappa(G)$. □

As you should expect from the definition, there are graphs without a cutset: the complete graphs K_n. If G is connected but not a K_n, it has vertices v and w that are not adjacent, so removing the $n-2$ other vertices leaves a non-connected graph, and so the connectivity of G is at most $n-2$. Thus, only the complete graphs have connectivity $n-1$.

We do the same thing for edges:

DEFINITION 5.7.2 If a graph G is connected, any set of edges whose removal disconnects the graph is called a **cut**. G has edge connectivity k if there is a cut of size k but no smaller cut; the edge connectivity of a one-vertex graph is undefined. G is k-edge-

connected if the edge connectivity of G is at least k. The edge connectivity is denoted $\lambda(G)$. □

Any connected graph with at least two vertices can be disconnected by removing edges: by removing all edges incident with a single vertex the graph is disconnected. Thus, $\lambda(G) \leq \delta(G)$, where $\delta(G)$ is the minimum degree of any vertex in G. Note that $\delta(G) \leq n-1$, so $\lambda(G) \leq n-1$.

Removing a vertex also removes all of the edges incident with it, which suggests that $\kappa(G) \leq \lambda(G)$. This turns out to be true, though not as easy as you might hope. We write $G - v$ to mean G with vertex v removed, and $G - \{v_1, v_2, \ldots, v_k\}$ to mean G with all of $\{v_1, v_2, \ldots, v_k\}$ removed, and similarly for edges.

THEOREM 5.7.3 $\kappa(G) \leq \lambda(G)$.

Proof. We use induction on $\lambda = \lambda(G)$. If $\lambda = 0$, G is disconnected, so $\kappa = 0$. If $\lambda = 1$, removal of edge e with endpoints v and w disconnects G. If v and w are the only vertices of G, G is K_2 and has connectivity 1. Otherwise, removal of one of v and w disconnects G, so $\kappa = 1$.

As a special case we note that if $\lambda = n-1$ then $\delta = n-1$, so G is K_n and $\kappa = n-1$.

Now suppose $n-1 > \lambda = k > 1$, and removal of edges $e_1, e_2, \ldots, e_k$ disconnects G. Remove edge e_k with endpoints v and w to form G_1 with $\lambda(G_1) = k-1$. By the induction hypothesis, there are at most $k-1$ vertices $v_1, v_2, \ldots, v_j$ such that $G_2 = G_1 - \{v_1, v_2, \ldots, v_j\}$ is disconnected. Since $k < n-1$, $k-1 \leq n-3$, and so G_2 has at least 3 vertices.

If both v and w are vertices of G_2, and if adding e_k to G_2 produces a connected graph G_3, then removal of one of v and w will disconnect G_3 forming G_4, and $G_4 = G - \{v_1, v_2, \ldots, v_j, v\}$ or $G_4 = G - \{v_1, v_2, \ldots, v_j, w\}$, that is, removing at most k vertices disconnects G. If v and w are vertices of G_2 but adding e_k does not produce a connected graph, then removing $v_1, v_2, \ldots, v_j$ disconnects G. Finally, if at least one of v and w is not in G_2, then $G_2 = G - \{v_1, v_2, \ldots, v_j\}$ and the connectivity of G is less than k. So in all cases, $\kappa \leq k$. ■

Graphs that are 2-connected are particularly important, and the following simple theorem is useful.

THEOREM 5.7.4 If G has at least three vertices, the following are equivalent:

1. G is 2-connected
2. G is connected and has no cutpoint
3. For all distinct vertices u, v, w in G there is a path from u to v that does not contain w.

Proof. **1 ⇒ 3**: Since G is 2-connected, G with w removed is a connected graph G'. Thus, in G' there is a path from u to v, which in G is a path from u to v avoiding w.
3 ⇒ 2: If G has property 3 it is clearly connected. Suppose that w is a cutpoint, so that $G' = G - w$ is disconnected. Let u and v be vertices in two different components of G', so that no path connects them in G'. Then every path joining u to v in G must use w, a contradiction.
2 ⇒ 1: Since G has at least 3 vertices and has no cutpoint, its connectivity is at least 2, so it is 2-connected by definition. ■

There are other nice characterizations of 2-connected graphs.

THEOREM 5.7.5 If G has at least three vertices, then G is 2-connected if and only if every two vertices u and v are contained in a cycle.

Proof.
if: Suppose vertex w is removed from G, and consider any other vertices u and v. In G, u and v lie on a cycle; even if w also lies on this cycle, then u and v are still connected by a path when w is removed.

only if: Given u and v we want to show there is a cycle containing both. Let U be the set of vertices other than u that are contained in a cycle with u. First, we show that U is non-empty. Let w be adjacent to u, and remove the edge e between them. Since $\lambda(G) \geq \kappa(G) \geq 2$, $G - e$ is connected. Thus, there is a path from u to w; together with e this path forms a cycle containing u and w, so $w \in U$.

For a contradiction, suppose $v \notin U$. Let w be in U with $\mathrm{d}(w, v) \geq 1$ as small as possible, fix a cycle C containing u and w and a path P of length $\mathrm{d}(w, v)$ from w to v. By the previous theorem, there is a path Q from u to v that does not use w. Following this path from u, there is a last vertex x on the path that is also on the cycle containing u and w, and there is a first vertex y on the path, after x, with y also on the path from w to v (it is possible that $y = v$, but not that $y = w$); see figure 5.7.1. Now starting at u, proceeding on cycle C to x without using w, then from x to y on Q, then to w on P, and finally back to u on C, we see that $y \in U$. But y is closer to v than is w, a contradiction. Hence $v \in U$. ■

The following corollary is an easy restatement of this theorem.

COROLLARY 5.7.6 If G has at least three vertices, then G is 2-connected if and only if between every two vertices u and v there are two **internally disjoint** paths, that is, paths that share only the vertices u and v. ■

This version of the theorem suggests a generalization:

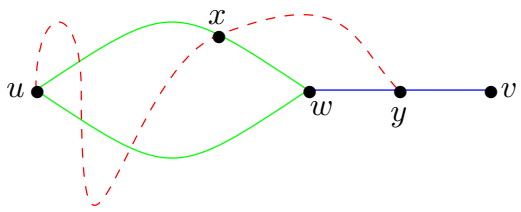


Figure 5.7.1 Point y closer to v than w is a contradiction; path Q is shown dashed. (See theorem 5.7.5.)

THEOREM 5.7.7 Menger's Theorem If G has at least $k+1$ vertices, then G is k-connected if and only if between every two vertices u and v there are k pairwise internally disjoint paths. □

We first prove Menger's original version of this, a "local" version.

DEFINITION 5.7.8 If v and w are non-adjacent vertices in G, $\kappa_G(v,w)$ is the smallest number of vertices whose removal separates v from w, that is, disconnects G leaving v and w in different components. A cutset that separates v and w is called a **separating set** for v and w. $p_G(v,w)$ is the maximum number of internally disjoint paths between v and w. □

THEOREM 5.7.9 If v and w are non-adjacent vertices in G, $\kappa_G(v,w) = p_G(v,w)$.

Proof. If there are k internally disjoint paths between v and w, then any set of vertices whose removal separates v from w must contain at least one vertex from each of the k paths, so $\kappa_G(v,w) \geq p_G(v,w)$.

To finish the proof, we show that there are $\kappa_G(v,w)$ internally disjoint paths between v and w. The proof is by induction on the number of vertices in G. If G has two vertices, G is not connected, and $\kappa_G(v,w) = p_G(v,w) = 0$. Now suppose G has $n > 2$ vertices and $\kappa_G(v,w) = k$.

Note that removal of either $N(v)$ or $N(w)$ separates v from w, so no separating set S of size k can properly contain $N(v)$ or $N(w)$. Now we address two cases:

Case 1: Suppose there is a set S of size k that separates v from w, and S contains a vertex not in $N(v)$ or $N(w)$. $G-S$ is disconnected, and one component G_1 contains v. Since S does not contain $N(v)$, G_1 has at least two vertices; let $X = V(G_1)$ and $Y = V(G) - S - X$. Since S does not contain $N(w)$, Y contains at least two vertices. Now we form two new graphs: Form H_X by starting with $G-Y$ and adding a vertex y adjacent to every vertex of S. Form H_Y by starting with $G-X$ and adding a vertex x adjacent to every vertex of S; see figure 5.7.2. Since X and Y each contain at least two vertices, H_X and H_Y are smaller than G, and so the induction hypothesis applies to them.

Clearly S separates v from y in H_X and w from x in H_Y. Moreover, any set that separates v from y in H_X separates v from w in G, so $\kappa_{H_X}(v, y) = \kappa_G(v, w) = k$. Similarly, $\kappa_{H_Y}(x, w) = \kappa_G(v, w) = k$. Hence, by the induction hypothesis, there are k internally disjoint paths from v to y in H_X and k internally disjoint paths from x to w in H_Y. Each of these paths uses one vertex of S; by eliminating x and y and joining the paths at the vertices of S, we produce k internally disjoint paths from v to w.

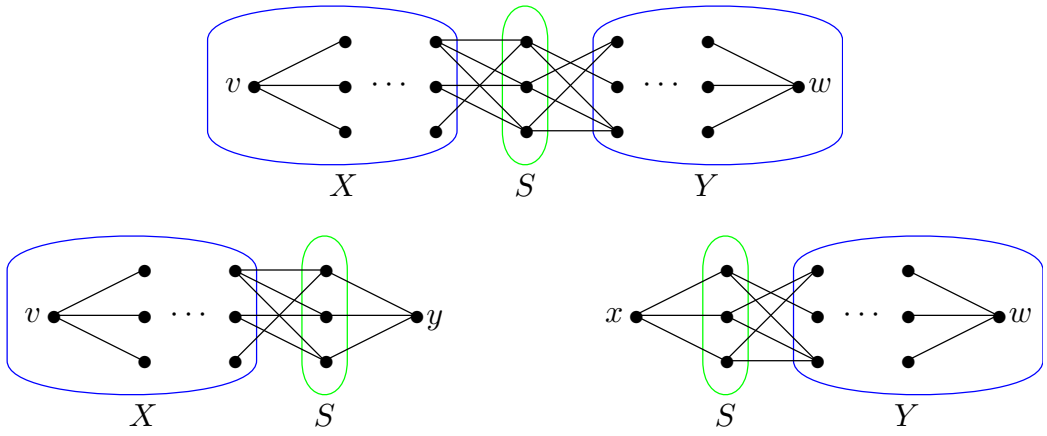


Figure 5.7.2 Case 1: Top figure is G, lower left is H_X, lower right is H_Y.

Case 2: Now we suppose that any set S separating v and w is a subset of $N(v) \cup N(w)$; pick such an S. If there is a vertex u not in $\{v, w\} \cup N(v) \cup N(w)$, consider $G - u$. This u is not in any set of size k that separates v from w, for if it were we would be in Case 1. Since S separates v from w in $G - u$, $\kappa_{G-u}(v, w) \leq k$. But if some smaller set S' separates v from w in $G - u$, then $S' \cup \{u\}$ separates v from w in G, a contradiction, so $\kappa_{G-u}(v, w) = k$. By the induction hypothesis, there are k internally disjoint paths from v to w in $G - u$ and hence in G.

We are left with $V(G) = \{v, w\} \cup N(v) \cup N(w)$. Suppose there is a vertex u in $N(v) \cap N(w)$. Then u is in every set that separates v from w, so $\kappa_{G-u} = k - 1$. By the induction hypothesis, there are $k - 1$ internally disjoint paths from v to w in $G - u$ and together with the path v, u, w, they comprise k internally disjoint paths from v to w in G.

Finally, suppose that $N(v) \cap N(w) = \emptyset$. Form a bipartite graph B with vertices $N(v) \cup N(w)$ and any edges of G that have one endpoint in $N(v)$ and the other in $N(w)$. Every set separating v from w in G must include one endpoint of every edge in B, that is, must be a vertex cover in B, and conversely, every vertex cover in B separates v from w in G. Thus, the minimum size of a vertex cover in B is k, and so there is a matching in B of size k, by theorem 4.5.6. The edges of this matching, together with the edges incident at v and w, form k internally disjoint paths from v to w in G. ■

Proof of Menger's Theorem (5.7.7)**.** Suppose first that between every two vertices v and w in G there are k internally disjoint paths. If G is not k-connected, the connectivity of G is at most $k-1$, and because G has at least $k+1$ vertices, there is a cutset S of G with size at most $k-1$. Let v and w be vertices in two different components of $G-S$; in G these vertices are joined by k internally disjoint paths. Since there is no path from v to w in $G-S$, each of these k paths contains a vertex of S, but this is impossible since S has size less than k, and the paths share no vertices other than v and w. This contradiction shows that G is k-connected.

Now suppose G is k-connected.

If v and w are not adjacent, $\kappa_G(v,w) \geq k$ and by the previous theorem there are $p_G(v,w) = \kappa_G(v,w)$ internally disjoint paths between v and w.

If v and w are connected by edge e, consider $G-e$. Suppose there is a separating set S for v and w with $|S| < k-1$, that is, $\kappa_{G-e}(v,w) < k-1$. S cannot be a cutset for G, so $G-S$ is connected. Then $G-e-S$ must have exactly two components, since $G-S$ is $G-e-S$ plus a single edge. $G-e-S$ has at least $k+1-(k-2)=3$ vertices, so one of the two components contains at least two vertices; without loss of generality, say u and w are in a single component. Then $G-(S\cup\{w\})$ is not connected, but $|S\cup\{w\}| < k$, contradicting the assumption that G is k-connected. Thus, $\kappa_{G-e}(v,w) \geq k-1$, so there are $k-1$ internally disjoint paths between v and w in $G-e$. Together with the path from v to w using e, this gives k internally disjoint paths between v and w in G, as desired. ■

• • •

We return briefly to 2-connectivity. The next theorem can sometimes be used to provide the induction step in an induction proof.

THEOREM 5.7.10 The Handle Theorem Suppose G is 2-connected and K is a 2-connected proper subgraph of G. Then there are subgraphs L and H (the handle) of G such that L is 2-connected, L contains K, H is a simple path, L and H share exactly the endpoints of H, and G is the union of L and H.

Proof. Given G and K, let L be a maximal proper subgraph of G containing K. If $V(L) = V(G)$, let e be an edge not in L. Since L plus the edge e is 2-connected, it must be G, by the maximality of L. Hence H is the path consisting of e and its endpoints.

Suppose that v is in $V(G)$ but not $V(L)$. Let u be a vertex of L. Since G is 2-connected, there is a cycle containing v and u. Following the cycle from v to u, Let w be the first vertex in L. Continuing on the cycle from u to v, let x be the last vertex in L. Let P be the path continuing around the cycle: $(x, v_1, v_2, \ldots, v_k, v = v_{k+1}, v_{k+2}, \ldots, v_m, w)$. If $x \neq w$, let $H = P$. Since L together with H is 2-connected, it is G, as desired.

If $x = w$ then $x = w = u$. Let y be a vertex of L other than u. Since G is 2-connected, there is a path P_1 from v to y that does not include u. Let v_j be the last vertex on P_1 that is in $\{v_1, \ldots, v, \ldots, v_m\}$; without loss of generality, suppose $j \geq k+1$. Then let H be the path $(u, v_1, \ldots, v = v_{k+1}, \ldots, v_j, \ldots, y)$, where from v_j to y we follow path P_1. Now $L \cup H$ is a 2-connected subgraph of G, but it is not G, as it does not contain the edge $\{u, v_m\}$, contradicting the maximality of L. Thus $x \neq w$. ■

A graph that is not connected consists of connected components. In a theorem reminiscent of this, we see that connected graphs that are not 2-connected are constructed from 2-connected subgraphs and bridges.

DEFINITION 5.7.11 A **block** in a graph G is a maximal induced subgraph on at least two vertices without a cutpoint. □

As usual, maximal here means that the induced subgraph B cannot be made larger by adding vertices or edges (while retaining the desired property, in this case, no cutpoints). A block is either a 2-connected induced subgraph or a single edge together with its endpoints. Blocks are useful in large part because of this theorem:

THEOREM 5.7.12 The blocks of G partition the edges.

Proof. We need to show that every edge is in exactly one block. If an edge is in no 2-connected induced subgraph of G, then, together with its endpoints, it is itself a block. Thus, every edge is in some block.

Now suppose that B_1 and B_2 are distinct blocks. This implies that neither is a subgraph of the other, by the maximality condition. Hence, the induced subgraph $G[V(B_1) \cup V(B_2)]$ is larger than either of B_1 and B_2. Suppose B_1 and B_2 share an edge, so that they share the endpoints of this edge, say u and v. Supppose w is a vertex in $V(B_1) \cup V(B_2)$. Since $B_1 - w$ and $B_2 - w$ are connected, so is $G[(V(B_1) \cup V(B_2)) \backslash \{w\}]$, because either u or v is in $(V(B_1) \cup V(B_2)) \backslash \{w\}$. Thus $G[V(B_1) \cup V(B_2)]$ has no cutpoint but strictly contains B_1 and B_2, contradicting the maximality property of blocks. Thus, every edge is in at most one block. ■

If G has a single block, it is either K_2 or is 2-connected, and any 2-connected graph has a single block.

THEOREM 5.7.13 If G is connected but not 2-connected, then every vertex that is in two blocks is a cutpoint of G.

Proof. Suppose w is in B_1 and B_2, but $G - w$ is connected. Then there is a path $v_1, v_2, \ldots, v_k$ in $G - w$, with $v_1 \in B_1$ and $v_k \in B_2$. But then $G[V(B_1) \cup V(B_2) \cup \{v_1, v_2, \ldots, v_k\}]$ has no cutpoint and contains both B_1 and B_2, a contradiction. ■

Exercises 5.7.

1. Suppose a simple graph G on $n \geq 2$ vertices has at least $\dfrac{(n-1)(n-2)}{2} + 1$ edges. Prove that G is connected.

2. Suppose a general graph G has exactly two odd-degree vertices, v and w. Let G' be the graph created by adding an edge joining v to w. Prove that G' is connected if and only if G is connected.

3. Suppose G is simple with degree sequence $d_1 \leq d_2 \leq \cdots \leq d_n$, and for $k \leq n - d_n - 1$, $d_k \geq k$. Show G is connected.

4. Recall that a graph is k-regular if all the vertices have degree k. What is the smallest integer k that makes this true:

> If G is simple, has n vertices, $m \geq k$, and G is m-regular, then G is connected.

(Of course k depends on n.)

5. Suppose G has at least one edge. Show that G is 2-connected if and only if for all vertices v and edges e there is a cycle containing v and e.

6. Find a simple graph with $\kappa(G) < \lambda(G) < \delta(G)$.

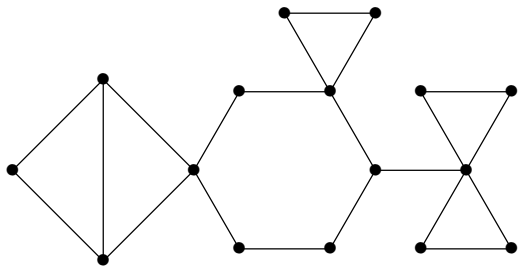
7. Suppose $\lambda(G) = k > 0$. Show that there are sets of vertices U and V that partition the vertices of G, and such that there are exactly k edges with one endpoint in U and one endpoint in V.

8. Find $\lambda(K_{m,n})$, where both m and n are at least 1. ($K_{m,n}$ is the complete bipartite graph on m and n vertices: the parts have m and n vertices, and every pair of vertices, one from each part, is connected by an edge.)

9. Suppose G is a connected graph. The **block-cutpoint graph** of G, $BC(G)$ is formed as follows: Let vertices $c_1, c_2, \ldots, c_k$ be the cutpoints of G, and let the blocks of G be $B_1, \ldots, B_l$. The vertices of $BC(G)$ are $c_1, \ldots, c_k, B_1, \ldots, B_l$. Add an edge $\{B_i, c_j\}$ if and only if $c_j \in B_i$. Show that the block-cutpoint graph is a tree.

Note that a cutpoint is contained in at least two blocks, so that all pendant vertices of the block-cutpoint graph are blocks. These blocks are called **endblocks**.

10. Draw the block-cutpoint graph of the graph below.



11. Show that the complement of a disconnected graph is connected. Is the complement of a connected graph always disconnected? (The complement $\overline{G}$ of graph G has the same vertices as G, and $\{v, w\}$ is an edge of $\overline{G}$ if and only if it is not an edge of G.)

5.8 Graph Coloring

As we briefly discussed in section 1.1, the most famous graph coloring problem is certainly the map coloring problem, proposed in the nineteenth century and finally solved in 1976.

DEFINITION 5.8.1 A **proper coloring** of a graph is an assignment of colors to the vertices of the graph so that no two adjacent vertices have the same color. □

Usually we drop the word "proper" unless other types of coloring are also under discussion. Of course, the "colors" don't have to be actual colors; they can be any distinct labels—integers, for example. If a graph is not connected, each connected component can be colored independently; except where otherwise noted, we assume graphs are connected. We also assume graphs are simple in this section.

Graph coloring has many applications in addition to its intrinsic interest.

EXAMPLE 5.8.2 If the vertices of a graph represent academic classes, and two vertices are adjacent if the corresponding classes have people in common, then a coloring of the vertices can be used to schedule class meetings. Here the colors would be schedule times, such as 8MWF, 9MWF, 11TTh, etc. □

EXAMPLE 5.8.3 If the vertices of a graph represent radio stations, and two vertices are adjacent if the stations are close enough to interfere with each other, a coloring can be used to assign non-interfering frequencies to the stations. □

EXAMPLE 5.8.4 If the vertices of a graph represent traffic signals at an intersection, and two vertices are adjacent if the corresponding signals cannot be green at the same time, a coloring can be used to designate sets of signals than can be green at the same time. □

Graph coloring is closely related to the concept of an **independent set**.

DEFINITION 5.8.5 A set S of vertices in a graph is independent if no two vertices of S are adjacent. □

If a graph is properly colored, the vertices that are assigned a particular color form an independent set. Given a graph G it is easy to find a proper coloring: give every vertex a different color. Clearly the interesting quantity is the minimum number of colors required for a coloring. It is also easy to find independent sets: just pick vertices that are mutually non-adjacent. A single vertex set, for example, is independent, and usually finding larger independent sets is easy. The interesting quantity is the maximum size of an independent set.

DEFINITION 5.8.6 The **chromatic number** of a graph G is the minimum number of colors required in a proper coloring; it is denoted $\chi(G)$. The **independence number** of G is the maximum size of an independent set; it is denoted $\alpha(G)$. □

The natural first question about these **graphical parameters** is: how small or large can they be in a graph G with n vertices. It is easy to see that

$$1 \leq \chi(G) \leq n$$
$$1 \leq \alpha(G) \leq n$$

and that the limits are all attainable: A graph with no edges has chromatic number 1 and independence number n, while a complete graph has chromatic number n and independence number 1. These inequalities are thus not very interesting. We will see some that are more interesting.

Another natural question: What is the relation between the chromatic number of a graph G and chromatic number of a subgraph of G? This too is simple, but quite useful at times.

THEOREM 5.8.7 If H is a subgraph of G, $\chi(H) \leq \chi(G)$.

Proof. Any coloring of G provides a proper coloring of H, simply by assigning the same colors to vertices of H that they have in G. This means that H can be colored with $\chi(G)$ colors, perhaps even fewer, which is exactly what we want. ■

Often this fact is interesting "in reverse". For example, if G has a subgraph H that is a complete graph K_m, then $\chi(H) = m$ and so $\chi(G) \geq m$. A subgraph of G that is a complete graph is called a **clique**, and there is an associated graphical parameter.

DEFINITION 5.8.8 The **clique number** of a graph G is the largest m such that K_m is a subgraph of G. □

It is tempting to speculate that the *only* way a graph G could require m colors is by having such a subgraph. This is false; graphs can have high chromatic number while having low clique number; see figure 5.8.1. It is easy to see that this graph has $\chi \geq 3$, because there are many 3-cliques in the graph. In general it can be difficult to show that a graph cannot be colored with a given number of colors, but in this case it is easy to see that the graph cannot in fact be colored with three colors, because so much is "forced". Suppose the graph can be colored with 3 colors. Starting at the left if vertex v_1 gets color 1, then v_2 and v_3 must be colored 2 and 3, and vertex v_4 must be color 1. Continuing, v_{10} must be color 1, but this is not allowed, so $\chi > 3$. On the other hand, since v_{10} can be colored 4, we see $\chi = 4$.

Paul Erdős showed in 1959 that there are graphs with arbitrarily large chromatic number and arbitrarily large **girth** (the girth is the size of the smallest cycle in a graph).

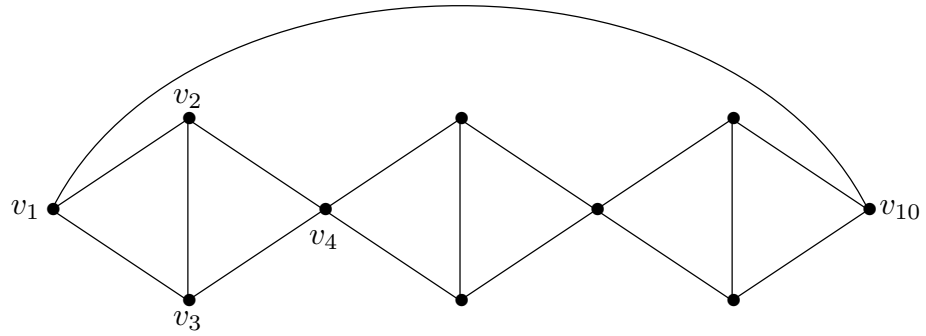


Figure 5.8.1 A graph with clique number 3 and chromatic number 4.

This is much stronger than the existence of graphs with high chromatic number and low clique number.

Bipartite graphs with at least one edge have chromatic number 2, since the two parts are each independent sets and can be colored with a single color. Conversely, if a graph can be 2-colored, it is bipartite, since all edges connect vertices of different colors. This means it is easy to identify bipartite graphs: Color any vertex with color 1; color its neighbors color 2; continuing in this way will or will not successfully color the whole graph with 2 colors. If it fails, the graph cannot be 2-colored, since all choices for vertex colors are forced.

If a graph is properly colored, then each **color class** (a color class is the set of all vertices of a single color) is an independent set.

THEOREM 5.8.9 In any graph G on n vertices, $\dfrac{n}{\alpha} \leq \chi$.

Proof. Suppose G is colored with χ colors. Since each color class is independent, the size of any color class is at most α. Let the color classes be $V_1, V_2, \ldots, V_\chi$. Then

$$n = \sum_{i=1}^{\chi} |V_i| \leq \chi\alpha,$$

as desired. ■

We can improve the upper bound on $\chi(G)$ as well. In any graph G, $\Delta(G)$ is the maximum degree of any vertex.

THEOREM 5.8.10 In any graph G, $\chi \leq \Delta + 1$.

Proof. We show that we can always color G with $\Delta + 1$ colors by a simple **greedy algorithm**: Pick a vertex v_n, and list the vertices of G as $v_1, v_2, \ldots, v_n$ so that if $i < j$, $\mathrm{d}(v_i, v_n) \geq \mathrm{d}(v_j, v_n)$, that is, we list the vertices farthest from v_n first. We use integers

$1, 2, \ldots, \Delta + 1$ as colors. Color v_1 with 1. Then for each v_i in order, color v_i with the smallest integer that does not violate the proper coloring requirement, that is, which is different than the colors already assigned to the neighbors of v_i. For $i < n$, we claim that v_i is colored with one of $1, 2, \ldots, \Delta$.

This is certainly true for v_1. For $1 < i < n$, v_i has at least one neighbor that is not yet colored, namely, a vertex closer to v_n on a shortest path from v_n to v_i. Thus, the neighbors of v_i use at most $\Delta - 1$ colors from the colors $1, 2, \ldots, \Delta$, leaving at least one color from this list available for v_i.

Once $v_1, \ldots, v_{n-1}$ have been colored, all neighbors of v_n have been colored using the colors $1, 2, \ldots, \Delta$, so color $\Delta + 1$ may be used to color v_n. ■

Note that if $\mathrm{d}(v_n) < \Delta$, even v_n may be colored with one of the colors $1, 2, \ldots, \Delta$. Since the choice of v_n was arbitrary, we may choose v_n so that $\mathrm{d}(v_n) < \Delta$, unless all vertices have degree Δ, that is, if G is regular. Thus, we have proved somewhat more than stated, namely, that any graph G that is not regular has $\chi \leq \Delta$. (If instead of choosing the particular order of $v_1, \ldots, v_n$ that we used we were to list them in arbitrary order, even vertices other than v_n might require use of color $\Delta + 1$. This gives a slightly simpler proof of the stated theorem.) We state this as a corollary.

COROLLARY 5.8.11 If G is not regular, $\chi \leq \Delta$. ■

There are graphs for which $\chi = \Delta + 1$: any cycle of odd length has $\Delta = 2$ and $\chi = 3$, and K_n has $\Delta = n - 1$ and $\chi = n$. Of course, these are regular graphs. It turns out that these are the only examples, that is, if G is not an odd cycle or a complete graph, then $\chi(G) \leq \Delta(G)$.

THEOREM 5.8.12 Brooks's Theorem If G is a graph other than K_n or C_{2n+1}, $\chi \leq \Delta$. ■

The greedy algorithm will not always color a graph with the smallest possible number of colors. Figure 5.8.2 shows a graph with chromatic number 3, but the greedy algorithm uses 4 colors if the vertices are ordered as shown.

In general, it is difficult to compute $\chi(G)$, that is, it takes a large amount of computation, but there is a simple algorithm for graph coloring that is not fast. Suppose that v and w are non-adjacent vertices in G. Denote by $G + \{v, w\} = G + e$ the graph formed by adding edge $e = \{v, w\}$ to G. Denote by G/e the graph in which v and w are "identified", that is, v and w are replaced by a single vertex x adjacent to all neighbors of v and w. (But note that we do not introduce multiple edges: if u is adjacent to both v and w in G, there will be a single edge from x to u in G/e.)

Consider a proper coloring of G in which v and w are different colors; then this is a proper coloring of $G + e$ as well. Also, any proper coloring of $G + e$ is a proper coloring of

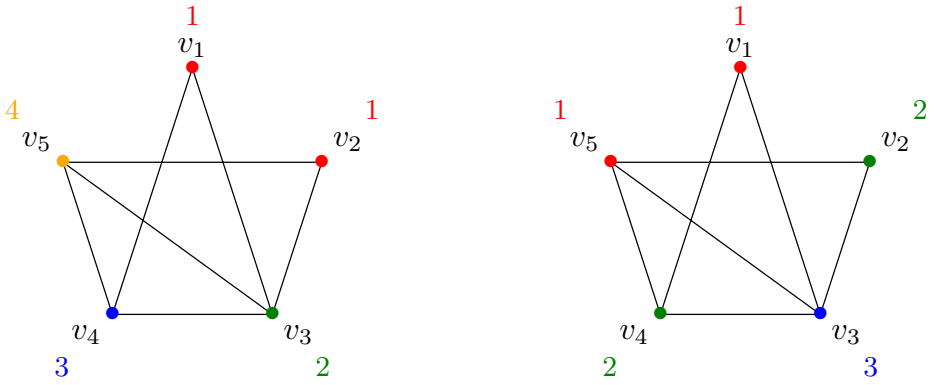


Figure 5.8.2 A greedy coloring on the left and best coloring on the right.

G in which v and w have different colors. So a coloring of $G+e$ with the smallest possible number of colors is a best coloring of G in which v and w have different colors, that is, $\chi(G+e)$ is the smallest number of colors needed to color G so that v and w have different colors.

If G is properly colored and v and w have the same color, then this gives a proper coloring of G/e, by coloring x in G/e with the same color used for v and w in G. Also, if G/e is properly colored, this gives a proper coloring of G in which v and w have the same color, namely, the color of x in G/e. Thus, $\chi(G/e)$ is the smallest number of colors needed to properly color G so that v and w are the same color.

The upshot of these observations is that $\chi(G) = \min(\chi(G+e), \chi(G/e))$. This algorithm can be applied recursively, that is, if $G_1 = G+e$ and $G_2 = G/e$ then $\chi(G_1) = \min(\chi(G_1+e), \chi(G_1/e))$ and $\chi(G_2) = \min(\chi(G_2+e), \chi(G_2/e))$, where of course the edge e is different in each graph. Continuing in this way, we can eventually compute $\chi(G)$, provided that eventually we end up with graphs that are "simple" to color. Roughly speaking, because G/e has fewer vertices, and $G+e$ has more edges, we must eventually end up with a complete graph along all branches of the computation. Whenever we encounter a complete graph K_m it has chromatic number m, so no further computation is required along the corresponding branch. Let's make this more precise.

THEOREM 5.8.13 The algorithm above correctly computes the chromatic number in a finite amount of time.

Proof. Suppose that a graph G has n vertices and m edges. The number of pairs of non-adjacent vertices is $\text{na}(G) = \binom{n}{2} - m$. The proof is by induction on na.

If $\text{na}(G) = 0$ then G is a complete graph and the algorithm terminates immediately.

Now we note that $\text{na}(G+e) < \text{na}(G)$ and $\text{na}(G/e) < \text{na}(G)$:

$$\text{na}(G+e) = \binom{n}{2} - (m+1) = \text{na}(G) - 1$$

and

$$\text{na}(G/e) = \binom{n-1}{2} - (m-c),$$

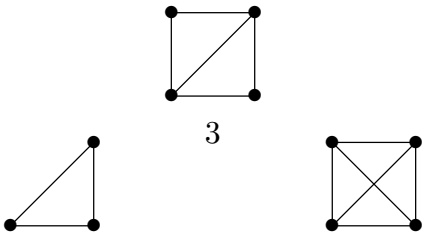
where c is the number of neighbors that v and w have in common. Then

$$\begin{aligned}
\text{na}(G/e) &= \binom{n-1}{2} - m + c \\
&\leq \binom{n-1}{2} - m + n - 2 \\
&= \frac{(n-1)(n-2)}{2} - m + n - 2 \\
&= \frac{n(n-1)}{2} - \frac{2(n-1)}{2} - m + n - 2 \\
&= \binom{n}{2} - m - 1 \\
&= \text{na}(G) - 1.
\end{aligned}$$

Now if $\text{na}(G) > 0$, G is not a complete graph, so there are non-adjacent vertices v and w. By the induction hypothesis the algorithm computes $\chi(G+e)$ and $\chi(G/e)$ correctly, and finally it computes $\chi(G)$ from these in one additional step. ■

While this algorithm is very inefficient, it is sufficiently fast to be used on small graphs with the aid of a computer.

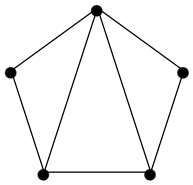
EXAMPLE 5.8.14 We illustrate with a very simple graph:



The chromatic number of the graph at the top is $\min(3,4) = 3$. (Of course, this is quite easy to see directly.) □

Exercises 5.8.

1. Suppose G has n vertices and chromatic number k. Prove that G has at least $\binom{k}{2}$ edges.
2. Find the chromatic number of the graph below by using the algorithm in this section. Draw all of the graphs $G+e$ and G/e generated by the alorithm in a "tree structure" with the complete graphs at the bottom, label each complete graph with its chromatic number, then propogate the values up to the original graph.



3. Show that $\chi(G - v)$ is either $\chi(G)$ or $\chi(G) - 1$.
4. Prove theorem 5.8.10 without assuming any particular properties of the order $v_1, \ldots, v_n$.
5. Prove theorem 5.8.12 as follows. By corollary 5.8.11 we need consider only regular graphs. Regular graphs of degree 2 are easy, so we consider only regular graphs of degree at least 3.

   If G is not 2-connected, show that the blocks of G may colored with $\Delta(G)$ colors, and then the colorings may be altered slightly so that they combine to give a proper coloring of G.

   If G is 2-connected, show that there are vertices u, v, w such that u is adjacent to both v and w, v and w are not adjacent, and $G - v - w$ is connected. Given such vertices, color v and w with color 1, then color the remaining vertices by a greedy algorithm similar to that in theorem 5.8.10, with u playing the role of v_n.

   To show the existence of u, v, w as required, let x be a vertex not adjacent to all other vertices. If $G - x$ is 2-connected, let $v = x$, let w be at distance 2 from v (justify this), and let a path of length 2 be v, u, w. Use theorem 5.7.4 to show that u, v, w have the required properties.

   If $G - x$ is not 2-connected, let $u = x$ and let v and w be (carefully chosen) vertices in two different endblocks of $G - x$. Show that u, v, w have the required properties.

   Brooks proved the theorem in 1941; this simpler proof is due to Lovász, 1975.

5.9 The Chromatic Polynomial

We now turn to the number of ways to color a graph G with k colors. Of course, if $k < \chi(G)$, this is zero. We seek a function $P_G(k)$ giving the number of ways to color G with k colors. Some graphs are easy to do directly.

EXAMPLE 5.9.1 If G is K_n, $P_G(k) = k(k-1)(k-2)\cdots(k-n+1)$, namely, the number of permutations of k things taken n at a time. Vertex 1 may be colored any of the k colors, vertex 2 any of the remaining $k-1$ colors, and so on. Note that when $k < n$, $P_G(k) = 0$. By exercise 5 in section 1.8, we may also write $P_G(k) = \sum_{i=0}^{n} s(n,i)k^i$. □

EXAMPLE 5.9.2 If G has n vertices and no edges, $P_G(k) = k^n$. □

Given P_G it is not hard to compute $\chi(G)$; for example, we could simply plug in the numbers $1, 2, 3, \ldots$ for k until $P_G(k)$ is non-zero. This suggests it will be difficult (that is, time consuming) to compute P_G. We can provide an easy mechanical procedure for the computation, quite similar to the algorithm we presented for computing $\chi(G)$.

Suppose G has edge $e = \{v, w\}$, and consider $P_{G-e}(k)$, the number of ways to color $G - e$ with k colors. Some of the colorings of $G - e$ are also colorings of G, but some are not, namely, those in which v and w have the same color. How many of these are there? From our discussion of the algorithm for $\chi(G)$ we know this is the number of colorings of G/e. Thus,

$$P_G(k) = P_{G-e}(k) - P_{G/e}(k).$$

Since $G - e$ and G/e both have fewer edges than G, we can compute P_G by applying this formula recursively. Ultimately, we need only compute P_G for graphs with no edges, which is easy, as in example 5.9.2.

Since $P_G(k) = k^n$ when G has no edges, it is then easy to see, and to prove by induction, that P_G is a polynomial.

THEOREM 5.9.3 For all G on n vertices, P_G is a polynomial of degree n, and P_G is called the **chromatic polynomial** of G.

Proof. The proof is by induction on the number of edges in G. When G has no edges, this is example 5.9.2.

Otherwise, by the induction hypothesis, P_{G-e} is a polynomial of degree n and $P_{G/e}$ is a polynomial of degree $n - 1$, so $P_G = P_{G-e} - P_{G/e}$ is a polynomial of degree n. ■

The chromatic polynomial of a graph has a number of interesting and useful properties, some of which are explored in the exercises.

Exercises 5.9.

1. Show that the leading coefficient of P_G is 1.
2. Suppose that G is not connected and has components $C_1, \ldots, C_k$. Show that $P_G = \prod_{i=1}^{k} P_{C_i}$.
3. Show that the constant term of $P_G(k)$ is 0. Show that the coefficient of k in $P_G(k)$ is non-zero if and only if G is connected.
4. Show that the coefficient of k^{n-1} in P_G is -1 times the number of edges in G.
5. Show that G is a tree if and only if $P_G(k) = k(k-1)^{n-1}$.
6. Find the chromatic polynomial of K_n with one edge removed.
7. Find the chromatic polynomial of the cycle C_n, $n \geq 3$.

5.10 Coloring Planar Graphs

Now we return to the original graph coloring problem: coloring maps. As indicated in section 1.1, the map coloring problem can be turned into a graph coloring problem. Figure 5.10.1 shows the example from section 1.1.

Graphs formed from maps in this way have an important property: they are **planar**.

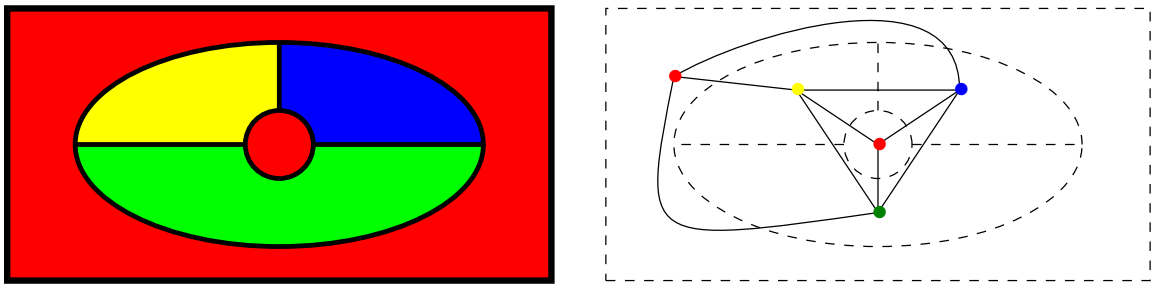


Figure 5.10.1 A map and its corresponding graph.

DEFINITION 5.10.1 A graph G is planar if it can be represented by a drawing in the plane so that no edges cross. □

Note that this definition only requires that some representation of the graph has no crossing edges. Figure 5.10.2 shows two representations of K_4; since in the second no edges cross, K_4 is planar.

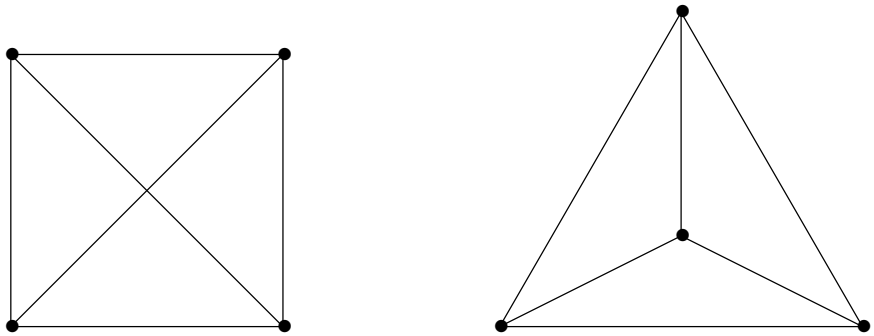


Figure 5.10.2 K_4 drawn in two ways; the second shows that it is planar.

The number of colors needed to properly color any map is now the number of colors needed to color any planar graph. This problem was first posed in the nineteenth century, and it was quickly conjectured that in all cases four colors suffice. This was finally proved in 1976 (see figure 5.10.3) with the aid of a computer. In 1879, Alfred Kempe gave a proof that was widely known, but was incorrect, though it was not until 1890 that this was noticed by Percy Heawood, who modified the proof to show that five colors suffice to color any planar graph. We will prove this Five Color Theorem, but first we need some other results. We assume all graphs are simple.

THEOREM 5.10.2 Euler's Formula Suppose G is a connected planar graph, drawn so that no edges cross, with n vertices and m edges, and that the graph divides the plane into r regions. Then

$$r = m - n + 2.$$

Figure 5.10.3 The postmark on University of Illinois mail after the Four Color Theorem was proved.

Proof. The proof is by induction on the number of edges. The base case is $m = n - 1$, the minimum number of edges in a connected graph on n vertices. In this case G is a tree, and contains no cycles, so the number of regions is 1, and indeed $1 = (n-1) - n + 2$.

Now suppose G has more than $n-1$ edges, so it has a cycle. Remove one edge from a cycle forming G', which is connected and has $r-1$ regions, n vertices, and $m-1$ edges. By the induction hypothesis $r - 1 = (m-1) - n + 2$, which becomes $r = m - n + 2$ when we add 1 to each side. ■

LEMMA 5.10.3 Suppose G is a simple connected planar graph, drawn so that no edges cross, with $n \geq 3$ vertices and m edges, and that the graph divides the plane into r regions. Then $m \leq 3n - 6$.

Proof. Let f_i be the number of edges that adjoin region number i; if the same region is on both sides of an edge, that edge is counted twice. We call the edges adjoining a region the boundary edges of the region. Since G is simple and $n \geq 3$, every region is bounded by at least 3 edges. Then $\sum_{i=1}^{r} f_i = 2m$, since each edge is counted twice, once for the region on each side of the edge. From $r = m - n + 2$ we get $3r = 3m - 3n + 6$, and because $f_i \geq 3$, $3r \leq \sum_{i=1}^{r} f_i = 2m$, so $3m - 3n + 6 \leq 2m$, or $m \leq 3n - 6$ as desired. ■

THEOREM 5.10.4 K_5 is not planar.

Proof. K_5 has 5 vertices and 10 edges, and $10 \not\leq 3 \cdot 5 - 6$, so by the lemma, K_5 is not planar. ■

LEMMA 5.10.5 If G is planar then G has a vertex of degree at most 5.

Proof. We may assume that G is connected (if not, work with a connected component of G). Suppose that $\mathrm{d}(v_i) > 5$ for all v_i. Then $2m = \sum_{i=1}^{n} \mathrm{d}(v_i) \geq 6n$. By lemma 5.10.3, $3n - 6 \geq m$ so $6n - 12 \geq 2m$. Thus $6n \leq 2m \leq 6n - 12$, a contradiction. ■

THEOREM 5.10.6 Five Color Theorem Every planar graph can be colored with 5 colors.

Proof. The proof is by induction on the number of vertices n; when $n \leq 5$ this is trivial.

Now suppose G is planar on more than 5 vertices; by lemma 5.10.5 some vertex v has degree at most 5. By the induction hypothesis, $G - v$ can be colored with 5 colors. Color the vertices of G, other than v, as they are colored in a 5-coloring of $G - v$. If $\mathrm{d}(v) \leq 4$, then v can be colored with one of the 5 colors to give a proper coloring of G with 5 colors. So we now suppose $\mathrm{d}(v) = 5$. If the five neighbors of v are colored with four or fewer of the colors, then again v can be colored to give a proper coloring of G with 5 colors.

Now we suppose that all five neighbors of v have a different color, as indicated in figure 5.10.4.

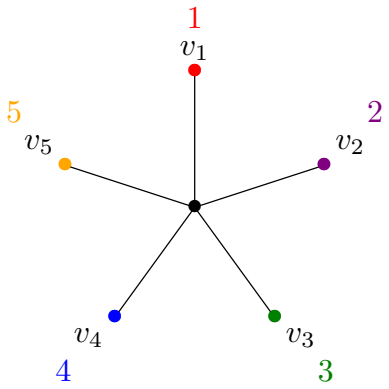


Figure 5.10.4 Five neighbors of v colored with 5 colors: v_1 is red, v_2 is purple, v_3 is green, v_4 is blue, v_5 is orange.

Suppose that in G there is a path from v_1 to v_3, and that the vertices along this path are alternately colored red and green; call such a path a red-green alternating path. Then together with v, this path makes a cycle with v_2 on the inside and v_4 on the outside, or vice versa. This means there cannot be a purple-blue alternating path from v_2 to v_4. Supposing that v_2 is inside the cycle, we change the colors of all vertices inside the cycle colored purple to blue, and all blue vertices are recolored purple. This is still a proper coloring of all vertices of G except v, and now no neighbor of v is purple, so by coloring v purple we obtain a proper coloring of G.

If there is no red-green alternating path from v_1 to v_3, then we recolor vertices as follows: Change the color of v_1 to green. Change all green neighbors of v_1 to red. Continue to change the colors of vertices from red to green or green to red until there are no conflicts, that is, until a new proper coloring is obtained. Because there is no red-green alternating path from v_1 to v_3, the color of v_3 will not change. Now no neighbor of v is colored red, so by coloring v red we obtain a proper coloring of G. ■

Exercises 5.10.

1. Show $K_{3,3}$ is not planar. (Prove a lemma like lemma 5.10.3 for bipartite graphs, then do something like the proof of theorem 5.10.4.) What is the chromatic number of $K_{3,3}$?

5.11 Directed Graphs

A **directed graph**, also called a **digraph**, is a graph in which the edges have a direction. This is usually indicated with an arrow on the edge; more formally, if v and w are vertices, an edge is an unordered pair $\{v, w\}$, while a directed edge, called an **arc**, is an ordered pair (v, w) or (w, v). The arc (v, w) is drawn as an arrow from v to w. If a graph contains both arcs (v, w) and (w, v), this is not a "multiple edge", as the arcs are distinct. It is possible to have multiple arcs, namely, an arc (v, w) may be included multiple times in the multiset of arcs. As before, a digraph is called simple if there are no loops or multiple arcs.

We denote by E_v^- the set of all arcs of the form (w, v), and by E_v^+ the set of arcs of the form (v, w). The **indegree** of v, denoted $\mathrm{d}^-(v)$, is the number of arcs in E_v^-, and the **outdegree**, $\mathrm{d}^+(v)$, is the number of arcs in E_v^+. If the vertices are $v_1, v_2, \ldots, v_n$, the degrees are usually denoted $d_1^-, d_2^-, \ldots, d_n^-$ and $d_1^+, d_2^+, \ldots, d_n^+$. Note that both $\sum_{i=0}^n \mathrm{d}_i^-$ and $\sum_{i=0}^n \mathrm{d}_i^+$ count the number of arcs exactly once, and of course $\sum_{i=0}^n \mathrm{d}_i^- = \sum_{i=0}^n \mathrm{d}_i^+$. A **walk** in a digraph is a sequence $v_1, e_1, v_2, e_2, \ldots, v_{k-1}, e_{k-1}, v_k$ such that $e_k = (v_i, v_{i+1})$; if $v_1 = v_k$, it is a closed walk or a circuit. A **path** in a digraph is a walk in which all vertices are distinct. It is not hard to show that, as for graphs, if there is a walk from v to w then there is a path from v to w.

Many of the topics we have considered for graphs have analogues in digraphs, but there are many new topics as well. We will look at one particularly important result in the latter category.

DEFINITION 5.11.1 A **network** is a digraph with a designated **source** s and **target** $t \neq s$. In addition, each arc e has a positive capacity, $c(e)$. □

Networks can be used to model transport through a physical network, of a physical quantity like oil or electricity, or of something more abstract, like information.

DEFINITION 5.11.2 A **flow** in a network is a function f from the arcs of the digraph to $\mathbb{R}$, with $0 \leq f(e) \leq c(e)$ for all e, and such that

$$\sum_{e \in E_v^+} f(e) = \sum_{e \in E_v^-} f(e),$$

for all v other than s and t. □

We wish to assign a value to a flow, equal to the net flow out of the source. Since the substance being transported cannot "collect" or "originate" at any vertex other than s and t, it seems reasonable that this value should also be the net flow into the target.

Before we prove this, we introduce some new notation. Suppose that U is a set of vertices in a network, with $s \in U$ and $t \notin U$. Let $\overrightarrow{U}$ be the set of arcs (v, w) with $v \in U$, $w \notin U$, and $\overleftarrow{U}$ be the set of arcs (v, w) with $v \notin U$, $w \in U$.

THEOREM 5.11.3 For any flow f in a network, the net flow out of the source is equal to the net flow into the target, namely,

$$\sum_{e \in E_s^+} f(e) - \sum_{e \in E_s^-} f(e) = \sum_{e \in E_t^-} f(e) - \sum_{e \in E_t^+} f(e).$$

Proof. We will show first that for any U with $s \in U$ and $t \notin U$,

$$\sum_{e \in E_s^+} f(e) - \sum_{e \in E_s^-} f(e) = \sum_{e \in \overrightarrow{U}} f(e) - \sum_{e \in \overleftarrow{U}} f(e).$$

Consider the following:

$$S = \sum_{v \in U} \left(\sum_{e \in E_v^+} f(e) - \sum_{e \in E_v^-} f(e) \right).$$

The quantity

$$\sum_{e \in E_v^+} f(e) - \sum_{e \in E_v^-} f(e)$$

is zero except when $v = s$, by the definition of a flow. Thus, the entire sum S has value

$$\sum_{e \in E_s^+} f(e) - \sum_{e \in E_s^-} f(e).$$

On the other hand, we can write the sum S as

$$\sum_{v \in U} \sum_{e \in E_v^+} f(e) - \sum_{v \in U} \sum_{e \in E_v^-} f(e).$$

Every arc $e = (x, y)$ with both x and y in U appears in both sums, that is, in

$$\sum_{v \in U} \sum_{e \in E_v^+} f(e),$$

when $v = x$, and in

$$\sum_{v \in U} \sum_{e \in E_v^-} f(e),$$

when $v = y$, and so the flow in such arcs contributes 0 to the overall value. Thus, only arcs with exactly one endpoint in U make a non-zero contribution, so the entire sum reduces

to

$$\sum_{e\in\overrightarrow{U}} f(e) - \sum_{e\in\overleftarrow{U}} f(e).$$

Thus

$$\sum_{e\in E_s^+} f(e) - \sum_{e\in E_s^-} f(e) = S = \sum_{e\in\overrightarrow{U}} f(e) - \sum_{e\in\overleftarrow{U}} f(e),$$

as desired.

Now let U consist of all vertices except t. Then

$$\sum_{e\in E_s^+} f(e) - \sum_{e\in E_s^-} f(e) = \sum_{e\in\overrightarrow{U}} f(e) - \sum_{e\in\overleftarrow{U}} f(e) = \sum_{e\in E_t^-} f(e) - \sum_{e\in E_t^+} f(e),$$

finishing the proof. ■

DEFINITION 5.11.4 The **value** of a flow, denoted $\mathrm{val}(f)$, is $\sum_{e\in E_s^+} f(e) - \sum_{e\in E_s^-} f(e)$. A **maximum flow** in a network is any flow f whose value is the maximum among all flows. □

We next seek to formalize the notion of a "bottleneck", with the goal of showing that the maximum flow is equal to the amount that can pass through the smallest bottleneck.

DEFINITION 5.11.5 A **cut** in a network is a set C of arcs with the property that every path from s to t uses an arc in C, that is, if the arcs in C are removed from the network there is no path from s to t. The capacity of a cut, denoted $c(C)$, is

$$\sum_{e\in C} c(e).$$

A minimum cut is one with minimum capacity. A cut C is minimal if no cut is properly contained in C. □

Note that a minimum cut is a minimal cut. Clearly, if U is a set of vertices containing s but not t, then $\overrightarrow{U}$ is a cut.

LEMMA 5.11.6 Suppose C is a minimal cut. Then there is a set U containing s but not t such that $C = \overrightarrow{U}$.

Proof. Let U be the set of vertices v such that there is a path from s to v using no arc in C.

Suppose that $e = (v, w) \in C$. Since C is minimal, there is a path P from s to t using e but no other arc in C. Thus, there is a path from s to v using no arc of C, so $v \in U$. If there is a path from s to w using no arc of C, then this path followed by the portion of P

that begins with w is a walk from s to t using no arc in C. This implies there is a path from s to t using no arc in C, a contradiction. Thus $w \notin U$ and so $e \in \overrightarrow{U}$. Hence, $C \subseteq \overrightarrow{U}$.

Suppose that $e = (v, w) \in \overrightarrow{U}$. Then $v \in U$ and $w \notin U$, so every path from s to w uses an arc in C. Since $v \in U$, there is a path from s to v using no arc of C, and this path followed by e is a path from s to w. Hence the arc e must be in C, so $\overrightarrow{U} \subseteq C$.

We have now shown that $C = \overrightarrow{U}$. ■

Now we can prove a version of the important max-flow, min cut theorem.

THEOREM 5.11.7 Suppose in a network all arc capacities are integers. Then the value of a maximum flow is equal to the capacity of a minimum cut. Moreover, there is a maximum flow f for which all $f(e)$ are integers.

Proof. First we show that for any flow f and cut C, $\text{val}(f) \leq c(C)$. It suffices to show this for a minimum cut C, and by lemma 5.11.6 we know that $C = \overrightarrow{U}$ for some U. Using the proof of theorem 5.11.3 we have:

$$\text{val}(f) = \sum_{e \in \overrightarrow{U}} f(e) - \sum_{e \in \overleftarrow{U}} f(e) \leq \sum_{e \in \overrightarrow{U}} f(e) \leq \sum_{e \in \overrightarrow{U}} c(e) = c(\overrightarrow{U}).$$

Now if we find a flow f and cut C with $\text{val}(f) = c(C)$, it follows that f is a maximum flow and C is a minimum cut. We present an algorithm that will produce such an f and C.

Given a flow f, which may initially be the zero flow, $f(e) = 0$ for all arcs e, do the following:

0. Let $U = \{s\}$.

Repeat the next two steps until no new vertices are added to U.

1. If there is an arc $e = (v, w)$ with $v \in U$ and $w \notin U$, and $f(e) < c(e)$, add w to U.

2. If there is an arc $e = (v, w)$ with $v \notin U$ and $w \in U$, and $f(e) > 0$, add v to U.

When this terminates, either $t \in U$ or $t \notin U$. If $t \in U$, there is a sequence of distinct vertices $s = v_1, v_2, v_3, \ldots, v_k = t$ such that for each i, $1 \leq i < k$, either $e = (v_i, v_{i+1})$ is an arc with $f(e) < c(e)$ or $e = (v_{i+1}, v_i)$ is an arc with $f(e) > 0$. Update the flow by adding 1 to $f(e)$ for each of the former, and subtracting 1 from $f(e)$ for each of the latter. This new flow f' is still a flow: In the first case, since $f(e) < c(e)$, $f'(e) \leq c(e)$, and in the second case, since $f(e) > 0$, $f'(e) \geq 0$. It is straightforward to check that for each vertex v_i, $1 < i < k$, that

$$\sum_{e \in E^+_{v_i}} f'(e) = \sum_{e \in E^-_{v_i}} f'(e).$$

In addition, $\text{val}(f') = \text{val}(f) + 1$. Now rename f' to f and repeat the algorithm.

Eventually, the algorithm terminates with $t \notin U$ and flow f. This implies that for each $e = (v, w)$ with $v \in U$ and $w \notin U$, $f(e) = c(e)$, and for each $e = (v, w)$ with $v \notin U$ and $w \in U$, $f(e) = 0$. The capacity of the cut $\overrightarrow{U}$ is

$$\sum_{e \in \overrightarrow{U}} c(e).$$

The value of the flow f is

$$\sum_{e \in \overrightarrow{U}} f(e) - \sum_{e \in \overleftarrow{U}} f(e) = \sum_{e \in \overrightarrow{U}} c(e) - \sum_{e \in \overleftarrow{U}} 0 = \sum_{e \in \overrightarrow{U}} c(e).$$

Thus we have found a flow f and cut $\overrightarrow{U}$ such that

$$\text{val}(f) = c(\overrightarrow{U}),$$

as desired. ■

The max-flow, min-cut theorem is true when the capacities are any positive real numbers, though of course the maximum value of a flow will not necessarily be an integer in this case. It is somewhat more difficult to prove; a proof involves limits.

We have already proved that in a bipartite graph, the size of a maximum matching is equal to the size of a minimum vertex cover, theorem 4.5.6. This turns out to be essentially a special case of the max-flow, min-cut theorem.

COROLLARY 5.11.8 In a bipartite graph G, the size of a maximum matching is the same as the size of a minimum vertex cover.

Proof. Suppose the parts of G are $X = \{x_1, x_2, \ldots, x_k\}$ and $Y = \{y_1, y_2, \ldots, y_l\}$. Create a network as follows: introduce two new vertices s and t and arcs (s, x_i) for all i and (y_i, t) for all i. For each edge $\{x_i, y_j\}$ in G, let (x_i, y_j) be an arc. Let $c(e) = 1$ for all arcs e. Now the value of a maximum flow is equal to the capacity of a minimum cut.

Let C be a minimum cut. If (x_i, y_j) is an arc of C, replace it by arc (s, x_i). This is still a cut, since any path from s to t including (x_i, y_j) must include (s, x_i). Thus, we may suppose that C contains only arcs of the form (s, x_i) and (y_i, t). Now it is easy to see that

$$K = \{x_i | (s, x_i) \in C\} \cup \{y_i | (y_i, t) \in C\}$$

is a vertex cover of G with the same size as C.

Let f be a maximum flow such that $f(e)$ is an integer for all e, and $\text{val}(f) = c(C)$, which is possible by the max-flow, min-cut theorem. Consider the set of edges

$$M = \{\{x_i, y_j\} | f((x_i, y_j)) = 1\}.$$

If $\{x_i, y_j\}$ and $\{x_i, y_m\}$ are both in this set, then the flow out of vertex x_i is at least 2, but there is only one arc into x_i, (s, x_i), with capacity 1, contradicting the definition of a

flow. Likewise, if $\{x_i, y_j\}$ and $\{x_m, y_j\}$ are both in this set, then the flow into vertex y_j is at least 2, but there is only one arc out of y_j, (y_j, t), with capacity 1, also a contradiction. Thus M is a matching. Moreover, if $U = \{s, x_1, \ldots, x_k\}$ then the value of the flow is

$$\sum_{e \in \overrightarrow{U}} f(e) - \sum_{e \in \overleftarrow{U}} f(e) = \sum_{e \in \overrightarrow{U}} f(e) = |M| \cdot 1 = |M|.$$

Thus $|M| = \text{val}(f) = c(C) = |K|$, so we have found a matching and a vertex cover with the same size. This implies that M is a maximum matching and K is a minimum vertex cover. ■

Exercises 5.11.

1. Connectivity in digraphs turns out to be a little more complicated than connectivity in graphs. A digraph is connected if the underlying graph is connected. (The underlying graph of a digraph is produced by removing the orientation of the arcs to produce edges, that is, replacing each arc (v, w) by an edge $\{v, w\}$. Even if the digraph is simple, the underlying graph may have multiple edges.) A digraph is strongly connected if for every vertices v and w there is a walk from v to w. Give an example of a digraph that is connected but not strongly connected.
2. A digraph has an Euler circuit if there is a closed walk that uses every arc exactly once. Show that a digraph with no vertices of degree 0 has an Euler circuit if and only if it is connected and $\text{d}^+(v) = \text{d}^-(v)$ for all vertices v.
3. A tournament is an oriented complete graph. That is, it is a digraph on n vertices, containing exactly one of the arcs (v, w) and (w, v) for every pair of vertices. A Hamilton path is a walk that uses every vertex exactly once. Show that every tournament has a Hamilton path.
4. Interpret a tournament as follows: the vertices are players. If (v, w) is an arc, player v beat w. Say that v is a **champion** if for every other player w, either v beat w or v beat a player who beat w. Show that a player with the maximum number of wins is a champion. Find a 5-vertex tournament in which every player is a champion.

6

Pólya–Redfield Counting

We have talked about the number of ways to properly color a graph with k colors, given by the chromatic polynomial. For example, the chromatic polynomial for the graph in figure 6.0.1 is $k^4 - 4k^3 + 6k^2 - 3k$, and $f(2) = 2$. The two colorings are shown in the figure, but in an obvious sense they are the same coloring, since one can be turned into the other by simply rotating the graph. We will consider a slightly different sort of coloring problem, in which we count the "truly different" colorings of objects.

Figure 6.0.1 C_4 drawn as a square, colored in two ways.

Many of the "objects" we color will appear to be graphs, but we will usually be interested in them as geometric objects rather than graphs, and we will not require that adjacent vertices be different colors. This will simplify the problems; counting the number of different proper colorings of graphs can also be done, but it is more complicated.

So consider this problem: How many different ways are there to color the vertices of a regular pentagon with k colors? The number of ways to color the vertices of a fixed pentagon is k^5, but this includes many duplicates, that is, colorings that are really the same. But what do we mean by "the same" in this case? We might mean that two colorings are the same if we can rotate one to get the other. But what about the colorings in figure 6.0.2? Are they the same? Neither can be rotated to produce the other, but either

can be flipped or reflected through a vertical line to produce the other. In fact we are free to decide what "the same" means, but we will need to make sure that our requirements are consistent.

Figure 6.0.2 Two colorings of a pentagon.

As an example of what can go wrong if we're not careful, note that there are five lines through which the pentagon can be reflected onto itself. Suppose we want to consider colorings to be "the same" if one can be produced from the other by a reflection, but not if one can be obtained from the other by rotation. Surely if one coloring can be obtained by two reflections in a row from another, then these colorings should also be the same. But two reflections in a row equal a rotation, as shown in figure 6.0.3. So whenever we have some motions that identify two colorings, we are required to include all combinations of the motions as well. In addition, any time we include a motion, we must include the "inverse" motion. For example, if we say a rotation by 72° degrees produces a coloring that we consider to be the same, a rotation by −72° must be included as well (we may think of this as a rotation by 288°). Finally, since any coloring is the same as itself, we must always include the "trivial" motion, namely, doing nothing, or rotation by 0° if you prefer.

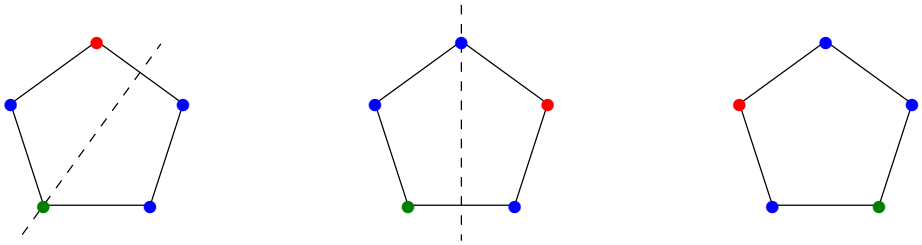


Figure 6.0.3 Two reflections equal a rotation.

6.1 Groups of Symmetries

The motions we want to consider can be thought of as permutations, that is, as bijections. For example, the rotation in figure 6.1.1 can be thought of as the function ϕ given by

$$\begin{aligned}\phi(1) &= 3\\ \phi(2) &= 4\\ \phi(3) &= 5\\ \phi(4) &= 1\\ \phi(5) &= 2,\end{aligned}$$

or more compactly we can write this function as $\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$.

Figure 6.1.1 The rotation $\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$.

As we would hope, doing two motions in a row corresponds to the compostion of the associated functions. For example, the reflection $\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}$ is shown in figure 6.1.2. Doing first the rotation of figure 6.1.1 and then this reflection is shown in figure 6.1.3, and this does indeed correspond to

$$\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&5&4&3&2\end{pmatrix}.$$

Figure 6.1.2 The reflection $\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}$.

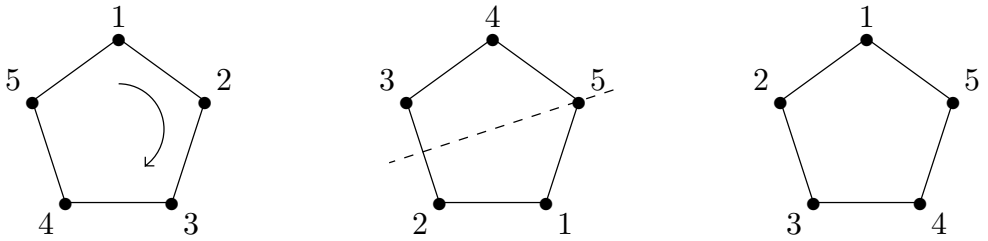


Figure 6.1.3 The compostion $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$.

With some restrictions, we may choose any permutations of the vertices as the allowable rearrangements giving colorings that are the same. We have discussed the restrictions in general terms; in terms of permuations we require the following: Suppose that G is a set of permutations that we wish to use to define the "same coloring" relation. Then the following must be true:

1. If ϕ and σ are in G, so is $\phi \circ \sigma$.
2. The identity permutation, id, is in G.
3. If $\phi \in G$, $\phi^{-1} \in G$.

DEFINITION 6.1.1 If G has the three properties above it is called a **group** of permutations. □

EXAMPLE 6.1.2 The group of all permutations of $\{1, 2, \ldots, n\}$ is denoted S_n, the **symmetric group** on n items. It satisfies the three required conditions by simple properties of bijections. □

In the case of the regular pentagon, there are a number of groups of permutations, but two are of primary interest. The five possible rotations (including the trivial rotation) form a group, the **cyclic group** of size 5. The total number of "rigid motions", that is, any combination of rotations and reflections that leave the pentagon superimposed on itself, is 10: Once the position of vertex 1 is established, the other vertices can increase from 1 either clockwise or counterclockwise. The rotations provide all of the former, and it is easy to check that the five reflections provide the counterclockwise positions. This is called a **dihedral group** and denoted D_5.

Suppose that G is some group of permutations of an object. If $\phi \in G$, then ϕ induces a function on the colorings of the object in a natural way, and we can use the same symbol ϕ to represent this function without confusion. If c is a coloring of the object, then $\phi(c)$ is the coloring that results by applying ϕ to the colored object, moving the colors with the object. See figure 6.1.4 for examples. We say that G **acts** on the set of colorings C.

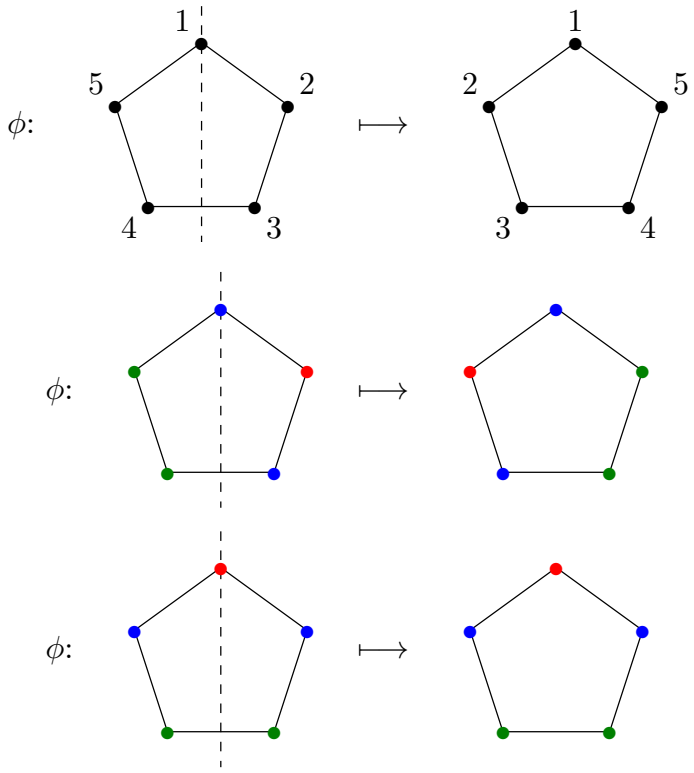


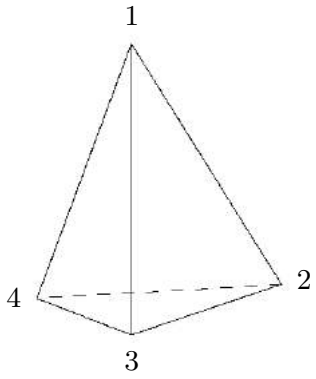
Figure 6.1.4 Some examples of an induced function on colorings.

If we apply all permutations in G to a coloring c, we get all the colorings that we consider to be the same as c modulo G. More formally, define $c_1 \sim c_2$ if there is a $\phi \in G$ such that $\phi(c_1) = c_2$; $\sim$ is an equivalence relation on the colorings. The equivalence classes, called **orbits** in this context, group colorings that are the same together. The number of truly different colorings that we want to count is then the number of orbits.

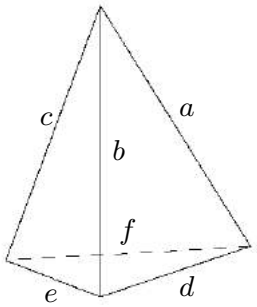
The total number of colorings of the pentagon with k colors is k^5. If all orbits were the same size, say s, then the number of orbits would be k^5/s. Unfortunately, this is not true. In figure 6.1.4 we see a coloring whose orbit has size at least 3, but the pentagon with all vertices colored red has orbit size 1.

Exercises 6.1.

1. Find the 12 permutations of the vertices of the regular tetrahedron corresponding to the 12 rigid motions of the regular tetrahedron. Use the labeling below.



2. Find the 12 permutations of the edges of the regular tetrahedron corresponding to the 12 rigid motions of the regular tetrahedron. Use the labeling below.



6.2 Burnside's Theorem

Burnside's Theorem will allow us to count the orbits, that is, the different colorings, in a variety of problems. We first need some lemmas.

If c is a coloring, $[c]$ is the orbit of c, that is, the equivalence class of c. Let $G(c)$ be the set of permutations in G that fix c, that is, those ϕ such that $\phi(c) = c$; the permutation in figure 6.1.4 fixes the coloring in the bottom row, for example.

LEMMA 6.2.1 $G(c)$ is a group of permutations.

Proof. We check the properties of a group from definition 6.1.1.

Suppose ϕ and σ both fix c; then $\phi(\sigma(c)) = \phi(c) = c$, so $\phi \circ \sigma$ fixes c and $\phi \circ \sigma \in G(c)$.

The identity permutation fixes all colorings, so $\mathrm{id} \in G(c)$.

If $\phi(c) = c$ then $\phi^{-1}(c) = \phi^{-1}(\phi(c)) = \mathrm{id}(c) = c$, so $\phi^{-1} \in G(c)$. ■

LEMMA 6.2.2 $|G| = |[c]| \cdot |G(c)|$.

Proof. For ϕ and σ in G, define $\phi \sim \sigma$ if $\sigma^{-1} \circ \phi \in G(c)$. This is an equivalence relation:

1. $\sigma^{-1} \circ \sigma$ is the identity function, which is in $G(c)$. Thus $\sigma \sim \sigma$, so the relation is reflexive.
2. If $\phi \sim \sigma$, $\sigma^{-1} \circ \phi \in G(c)$. Then $(\sigma^{-1} \circ \phi)^{-1} \in G(c)$, and $(\sigma^{-1} \circ \phi)^{-1} = \phi^{-1} \circ \sigma \in G(c)$, so $\sigma \sim \phi$ and $\sim$ is symmetric.

3. If $\phi \sim \sigma$ and $\sigma \sim \tau$, then $\sigma^{-1} \circ \phi \in G(c)$ and $\tau^{-1} \circ \sigma \in G(c)$, so $(\tau^{-1} \circ \sigma) \circ (\sigma^{-1} \circ \phi) \in G(c)$. Since $(\tau^{-1} \circ \sigma) \circ (\sigma^{-1} \circ \phi) = \tau^{-1} \circ \phi$, $\phi \sim \tau$, and $\sim$ is transitive.

Now we claim that the equivalence class of ϕ is $A = \{\phi \circ \sigma \mid \sigma \in G(c)\}$. First, suppose that $\sigma \in G(c)$; then $\phi^{-1} \circ \phi \circ \sigma = \sigma \in G(c)$, so $\phi \circ \sigma \sim \phi$ and $A \subseteq [\phi]$. Next, suppose $\phi \sim \tau$, so $\tau^{-1} \circ \phi = \gamma \in G(c)$. Then $\phi \circ \gamma^{-1} = \tau$, so $\tau \in A$ and $[\phi] \subseteq A$.

Now we show that each equivalence class is the same size as $G(c)$. Define $f: G(c) \to \{\phi \circ \sigma \mid \sigma \in G(c)\}$ by $f(\gamma) = \phi \circ \gamma$. If $f(\gamma_1) = f(\gamma_2)$, then

$$\begin{aligned} \phi \circ \gamma_1 &= \phi \circ \gamma_2 \\ \phi^{-1} \circ \phi \circ \gamma_1 &= \phi^{-1} \circ \phi \circ \gamma_2 \\ \gamma_1 &= \gamma_2 \end{aligned}$$

so f is 1–1. Since every $\phi \circ \gamma \in \{\phi \circ \sigma \mid \sigma \in G(c)\}$ is $f(\gamma)$, f is onto.

Thus the number of equivalence classes is $|G|/|G(c)|$.

Finally, we show that the number of equivalence classes is $|[c]|$. Let the set of equivalence classes in G be E, that is, $E = \{[\phi] \mid \phi \in G\}$. We define $g: [c] \to E$ and show that g is a bijection. Suppose $d \in [c]$, so $d = \sigma(c)$ for some $\sigma \in G$. Let $g(d) = [\sigma]$.

First, we show g is well-defined. If $d = \sigma_1(c) = \sigma_2(c)$, then $\sigma_2^{-1} \circ \sigma_1(c) = c$, so $\sigma_1 \sim \sigma_2$ and $[\sigma_1] = [\sigma_2]$, that is, $g(\sigma_1(c)) = g(\sigma_2(c))$.

Next, suppose $g(d_1) = g(d_2)$. This means that $d_1 = \sigma_1(c)$, $d_2 = \sigma_2(c)$, and $[\sigma_1] = [\sigma_2]$. Hence $\sigma_2^{-1} \circ \sigma_1(c) = c$, so $\sigma_1(c) = \sigma_2(c)$ and thus $d_1 = d_2$, so g is 1–1.

Suppose that $[\sigma] \in E$. Then $g(\sigma(c)) = [\sigma]$, so g is onto.

Thus we have

$$|[c]| = |E| = \frac{|G|}{|G(c)|}$$

and

$$|G(c)| \cdot |[c]| = |G|$$

as desired. ■

COROLLARY 6.2.3 If $c \sim d$ then $|G(c)| = |G(d)|$.

Proof. Since $c \sim d$, $[c] = [d]$, and

$$\begin{aligned} \frac{|G|}{|G(c)|} = |[c]| = |[d]| &= \frac{|G|}{|G(d)|} \\ |G(c)| &= |G(d)| \end{aligned}$$

■

DEFINITION 6.2.4 If group G acts on the colorings of an object and $\sigma \in G$, fix(σ) is the set of colorings that are fixed by σ. □

THEOREM 6.2.5 Burnside's Theorem If group G acts on the colorings of an object, the number of distinct colorings modulo G is

$$\frac{1}{|G|}\sum_{\sigma\in G}|\operatorname{fix}(\sigma)|.$$

Proof. Let C be the set of all colorings, and let $\mathcal{O}$ be the set of orbits. Let $c_1, c_2, \ldots, c_k$ be a list of colorings, one in each orbit, so that the orbits are $[c_1], [c_2], \ldots, [c_k]$. Consider the sum $\displaystyle\sum_{c\in C}|G(c)|$:

$$\begin{aligned}\sum_{c\in C}|G(c)| &= \sum_{i=1}^{k}\sum_{c\in[c_i]}|G(c)|\\ &= \sum_{i=1}^{k}\sum_{c\in[c_i]}|G(c_i)|\\ &= \sum_{i=1}^{k}\sum_{c\in[c_i]}\frac{|G|}{|[c_i]|}\\ &= \sum_{i=1}^{k}|[c_i]|\frac{|G|}{|[c_i]|}\\ &= \sum_{i=1}^{k}|G| = |G|\sum_{i=1}^{k}1 = |G||\mathcal{O}|.\end{aligned}$$

Then

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{c\in C}|G(c)|.$$

This already gives an interesting formula for $|\mathcal{O}|$, but it is unwieldy, since the number of colorings is typically quite large; indeed, since we typically want to compute the number of orbits for k colors, the number of colorings is not a fixed number.

With just a little more work we can fix this problem:

$$\begin{aligned}\sum_{c\in C}|G(c)| &= \sum_{c\in C}\sum_{\sigma\in G(c)}1\\ &= \sum_{\sigma\in G}\sum_{c\in\operatorname{fix}(\sigma)}1\\ &= \sum_{\sigma\in G}|\operatorname{fix}(\sigma)|.\end{aligned}$$

Now

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{\sigma\in G}|\operatorname{fix}(\sigma)|$$

as desired. ■

Since the group of permutations in a typical problem is fairly small, the sum in Burnside's Theorem is usually manageable. Moreover, we can make the task of computing $|\operatorname{fix}(\sigma)|$ fairly straightforward. Let's consider a particular example, the permutation of figure 6.1.4, shown again in figure 6.2.1. If we are using k colors, how many colorings of the pentagon are fixed by this permutation? Since the permutation swaps vertices 2 and 5, they must be the same color if ϕ is to fix the coloring. Likewise vertices 3 and 4 must be the same color; vertex 1 can be any color. Thus, the number of colorings fixed by ϕ is k^3. It is easy to see that every "flip" permutation of the pentagon is essentially the same, so for each of the five flip permutations, the size of $\operatorname{fix}(\sigma)$ is k^3.

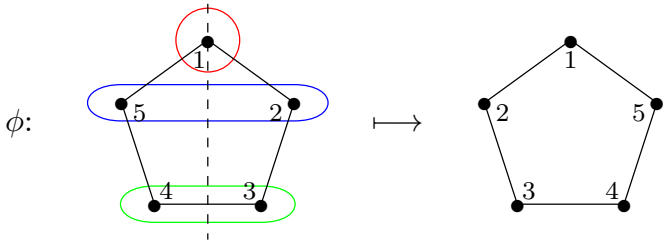


Figure 6.2.1 The cycles in a vertex permutation.

Every permutation can be written in **cycle form**: The permutation in figure 6.2.1, for example, is $(1)(2,5)(3,4)$. A cycle in this context is a sequence $(x_1, x_2, \ldots, x_k)$, meaning that $\phi(x_1) = x_2$, $\phi(x_2) = x_3$, and so on until $\phi(x_k) = x_1$. Following our reasoning above, the vertices in each cycle must be colored the same color, and the total number of colors fixed by ϕ is k^m, where m is the number of cycles.

Let's apply this to another permutation, shown in figure 6.2.2. This permutation consists of a single cycle, so every vertex must have the same color, and the number of colorings fixed by ϕ is k^1. All rotations of the pentagon consist of a single cycle except the trivial rotation, that is, the identity permutation. In cycle form, the identity permutation is $(1)(2)(3)(4)(5)$, so the number of colorings fixed by the identity is k^5. Putting everything together, we thus have

$$|\mathcal{O}| = \frac{1}{10}(k^5 + k + k + k + k + k^3 + k^3 + k^3 + k^3 + k^3) = \frac{1}{10}(k^5 + 5k^3 + 4k).$$

For example, the number of different 3-colorings is $(3^5 + 5 \cdot 3^3 + 4 \cdot 3)/10 = 39$.

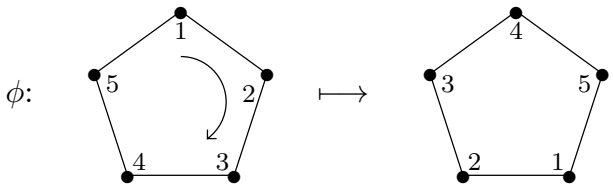


Figure 6.2.2 The permutation $(1, 3, 5, 2, 4)$ is a single cycle.

EXAMPLE 6.2.6 We find the number of distinct colorings of the vertices of a square with k colors, modulo D_4, the dihedral group of size 8. The elements of D_4 are the four rotations r_0, r_{90}, r_{180}, r_{270}, where r_i is the counterclockwise rotation by i degrees, and the four reflections f_H, f_V, f_D, f_A, as indicated in figure 6.2.3.

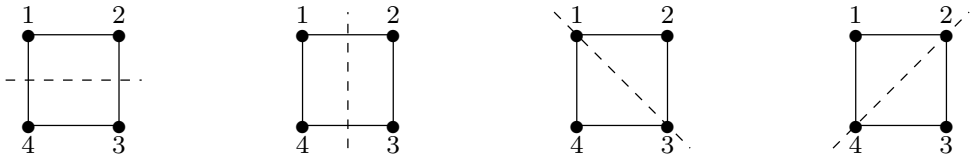


Figure 6.2.3 The reflection axes for f_H, f_V, f_D, and f_A.

In cycle notation these permutations are:

$$\begin{aligned} r_0 &= (1)(2)(3)(4) \\ r_{90} &= (1,4,3,2) \\ r_{180} &= (1,3)(2,4) \\ r_{270} &= (1,2,3,4) \\ f_H &= (1,4)(2,3) \\ f_V &= (1,2)(3,4) \\ f_D &= (1)(2,4)(3) \\ f_A &= (1,3)(2)(4). \end{aligned}$$

so the number of colorings is

$$f(k) = \frac{1}{8}(k^4 + k + k^2 + k + k^2 + k^2 + k^3 + k^3) = \frac{1}{8}(k^4 + 2k^3 + 3k^2 + 2k).$$

For example, $f(2) = 6$; the six colorings are shown in figure 6.2.4. □

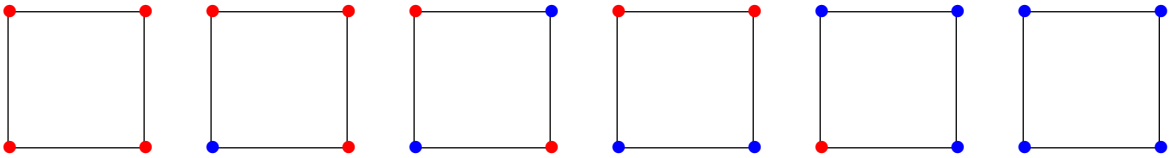


Figure 6.2.4 The six 2-colorings of the square.

EXAMPLE 6.2.7 Here is a more complicated example: how many different graphs are there on four vertices? In this case, of course, "different" means "non-isomorphic". We can interpret this as a coloring problem: Color the *edges* of the complete graph K_4 with

two colors, say black and white. The black edges form a graph; the white edges are the ones left out of the graph. The group G we need to consider is all permutations of the six edges of K_4 induced by a permutation of the vertices, so $|G| = 4! = 24$. All we need to know is the number of cycles in each permutation; we consider a number of cases.

Case 1. The identity permutation on the vertices induces the identity permutation on the edges, with 6 cycles, so the contribution to the sum is 2^6.

Case 2. A 4-cycle on the vertices induces a permutation of the edges consisting of one 4-cycle and one 2-cycle, that is, two cycles. There are $3! = 6$ 4-cycles on the vertices, so the contribution of all of these is $6 \cdot 2^2$.

Case 3. A permutation of the vertices consisting of a 3-cycle and a 1-cycle induces a permutation of the edges consisting of two 3-cycles. There are $4 \cdot 2 = 8$ such permutations of the vertices, so the contribution of all is $8 \cdot 2^2$.

Case 4. A permutation of the vertices consisting of two 2-cycles induces a permutation of the edges consisting of two 1-cycles and two 2-cycles. There are $\frac{1}{2}\binom{4}{2} = 3$ such permutations, so the contribution is $3 \cdot 2^4$.

Case 5. A permutation of the vertices consisting of a 2-cycle and two 1-cycles induces a permutation of the edges consisting of two 1-cycles and two 2-cycles. There are $\binom{4}{2} = 6$ such permutations, so the contribution is $6 \cdot 2^4$.

The number of distinct colorings, that is, the number of distinct graphs on four vertices, is

$$\frac{1}{24}(2^6 + 6 \cdot 2^2 + 8 \cdot 2^2 + 3 \cdot 2^4 + 6 \cdot 2^4) = \frac{1}{24}(264) = 11.$$

□

It is possible, though a bit difficult, to see that for n vertices the result is

$$f(n) = \sum_{\mathbf{j}} \prod_{k=1}^{n} \frac{1}{k^{j_k} j_k!} \prod_{k=1}^{\lfloor n/2 \rfloor} 2^{k j_{2k}} \prod_{k=1}^{\lfloor (n-1)/2 \rfloor} 2^{k j_{2k+1}} \prod_{k=1}^{\lfloor n/2 \rfloor} 2^{kC(j_k,2)} \prod_{1 \le r < s \le n-1} 2^{\gcd(r,s) j_r j_s} \qquad (6.2.1)$$

where the sum is over all partitions $\mathbf{j} = (j_1, j_2, \ldots, j_n)$ of n, that is, over all $\mathbf{j}$ such that $j_1 + 2j_2 + 3j_3 + \cdots + nj_n = n$, and $C(m, 2) = \binom{m}{2}$. With this formula and a computer it is easy to compute the number of graphs when n is not too large; for example, $f(5) = 34$, so there are 34 different five-vertex graphs.

In light of the forgoing discussion, we can restate theorem 6.2.5. If σ is a permutation, let $\#\sigma$ denote the number of cycles when σ is written in cycle form.

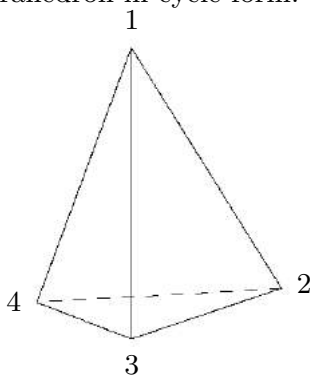
COROLLARY 6.2.8 If group G acts on the colorings of an object, the number of distinct colorings modulo G with k colors is

$$\frac{1}{|G|} \sum_{\sigma \in G} k^{\#\sigma}.$$

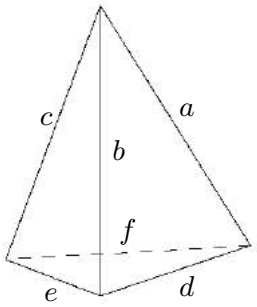
■

Exercises 6.2.

1. Write the 12 permutations of the vertices of the regular tetrahedron corresponding to the 12 rigid motions of the regular tetrahedron in cycle form. Use the labeling below.



2. Find the number of different colorings of the vertices of a regular tetrahedron with k colors, modulo the rigid motions.
3. Write the 12 permutations of the edges of the regular tetrahedron corresponding to the 12 rigid motions of the regular tetrahedron in cycle form. Use the labeling below.



4. Find the number of different colorings of the edges of a regular tetrahedron with k colors, modulo the rigid motions.
5. Find the number of non-isomorphic graphs on 5 vertices "by hand", that is, using the method of example 6.2.7.

6.3 Pólya-Redfield Counting

Suppose we are interested in a more detailed inventory of the colorings of an object, namely, instead of the total number of colorings we seek the number of colorings with a given number of each color. The method presented here was first published by J. Howard Redfield in 1927. In 1937 it was independently rediscovered by George Pólya, who then greatly popularized the result by applying it to many counting problems, in particular to the enumeration of chemical compounds.

EXAMPLE 6.3.1 How many distinct ways are there to color the vertices of a regular pentagon modulo D_5 so that one vertex is red, two are blue, and two are green?

We can approach this as before, that is, the answer is

$$\frac{1}{|D_5|}\sum_{\sigma\in D_5}|\operatorname{fix}(\sigma)|,$$

where $\operatorname{fix}(\sigma)$ now means the colorings with one red, two blues, and two greens that are fixed by σ. No longer can we use the simple expression of corollary 6.2.8.

The identity permutation fixes all colorings, so we need to know how many colorings of the pentagon use one red, two blues, and two greens. This is an easy counting problem: the number is $\binom{5}{2}\binom{3}{2} = 30$.

If σ is a non-trivial rotation, $|\operatorname{fix}(\sigma)| = 0$, since the only colorings fixed by a rotation have all vertices the same color.

If σ is a reflection, the single vertex fixed by σ must be red, and then the remaining 2-cycles are colored blue and green in one of two ways, so $|\operatorname{fix}(\sigma)| = 2$.

Thus, the number of distinct colorings is

$$\frac{1}{10}(30+0+0+0+0+2+2+2+2+2) = 4.$$

□

What we seek is a way to streamline this process, since in general the computations of $|\operatorname{fix}(\sigma)|$ can be tedious. We begin by recasting the formula of corollary 6.2.8.

DEFINITION 6.3.2 The **type** of a permutation $\sigma \in S_n$ is $\tau(\sigma) = (\tau_1(\sigma), \tau_2(\sigma), \ldots, \tau_n(\sigma))$, where $\tau_i(\sigma)$ is the number of i-cycles in the cycle form of σ. □

Note that $\sum_{i=1}^{n}\tau_i(\sigma) = \#\sigma$. Now instead of the simple

$$\frac{1}{|G|}\sum_{\sigma\in G}k^{\#\sigma}$$

let us write

$$\frac{1}{|G|}\sum_{\sigma\in G}x_1^{\tau_1(\sigma)}x_2^{\tau_2(\sigma)}\cdots x_n^{\tau_n(\sigma)}.$$

If we substitute $x_i = k$ for every i, we get the original form of the sum, but the new version carries more information about each σ.

Suppose we want to know the number of colorings fixed by some σ that use i reds and j blues, where of course $i+j=n$. Using ideas familiar from generating functions, consider the following expression:

$$(r+b)^{\tau_1(\sigma)}(r^2+b^2)^{\tau_2(\sigma)}\cdots(r^n+b^n)^{\tau_n(\sigma)}.$$

If we multiply out, we get a sum of terms of the form r^pb^q, each representing some particular way of coloring the vertices of cycles red and blue so that the total number of red vertices

is p and the number of blue vertices is q, and moreover this coloring will be fixed by σ. When we collect like terms, the coefficient of $r^i b^j$ is the number of colorings fixed by σ that use i reds and j blues. This means that the coefficient of $r^i b^j$ in

$$\sum_{\sigma \in G} (r+b)^{\tau_1(\sigma)} (r^2+b^2)^{\tau_2(\sigma)} \cdots (r^n+b^n)^{\tau_n(\sigma)}$$

is

$$\sum_{\sigma \in G} |\operatorname{fix}(\sigma)|$$

where $\operatorname{fix}(\sigma)$ is the set of colorings using i reds and j blues that are fixed by σ. Finally, then, the number of distinct colorings using i reds and j blues is this coefficient divided by $|G|$. This means that by multiplying out

$$\frac{1}{|G|} \sum_{\sigma \in G} (r+b)^{\tau_1(\sigma)} (r^2+b^2)^{\tau_2(\sigma)} \cdots (r^n+b^n)^{\tau_n(\sigma)}$$

and collecting like terms, we get a list of the number of distinct colorings using any combination of reds and blues, each the coefficient of a different term; we call this the **inventory** of colorings. If we substitute $r = 1$ and $b = 1$, we get the sum of the coefficients, namely, the total number of distinct colorings with two colors.

DEFINITION 6.3.3 The **cycle index** of G is

$$\mathcal{P}_G = \frac{1}{|G|} \sum_{\sigma \in G} \prod_{i=1}^{n} x_i^{\tau_i(\sigma)}.$$

□

EXAMPLE 6.3.4 Consider again example 6.2.6, in which we found the number of colorings of a square with two colors. The cycle index of D_4 is

$$\frac{1}{8}(x_1^4 + x_4^1 + x_2^2 + x_4^1 + x_2^2 + x_2^2 + x_1^2 x_2 + x_1^2 x_2) = \frac{1}{8}x_1^4 + \frac{1}{4}x_1^2 x_2 + \frac{3}{8}x_2^2 + \frac{1}{4}x_4.$$

Substituting as above gives

$$\frac{1}{8}(r+b)^4 + \frac{1}{4}(r+b)^2(r^2+b^2) + \frac{3}{8}(r^2+b^2)^2 + \frac{1}{4}(r^4+b^4) = r^4 + r^3 b + 2r^2 b^2 + r b^3 + b^4.$$

Thus there is one all red coloring, one with three reds and one blue, and so on, as shown in figure 6.2.4. □

There is nothing special about the use of two colors. If we want to use three colors, we substitute $r^i + b^i + g^i$ for x_i in the cycle index, and for k colors we substitute something like $c_1^i + c_2^i + c_3^i + \cdots + c_k^i$.

EXAMPLE 6.3.5 Let's do the number of 3-colorings of the square. Since we already have the cycle index, we need only substitute $x_i = r^i + b^i + g^i$ and expand. We get

$$\begin{aligned}\frac{1}{8}(r+b+g)^4 + \frac{1}{4}(r+b+g)^2(r^2+b^2+g^2) + \frac{3}{8}(r^2+b^2+g^2)^2 + \frac{1}{4}(r^4+b^4+g^4)\\ = b^4 + b^3g + b^3r + 2b^2g^2 + 2b^2gr + 2b^2r^2 + bg^3 + 2bg^2r + 2bgr^2 +\\ br^3 + g^4 + g^3r + 2g^2r^2 + gr^3 + r^4.\end{aligned}$$

So, for example, there are two squares with two blue vertices, one green, and one red, from the b^2gr term. □

EXAMPLE 6.3.6 Consider again example 6.2.7, in which we counted the number of four-vertex graphs. Following that example, we get

$$\mathcal{P}_G = \frac{1}{24}(x_1^6 + 6x_2x_4 + 8x_3^2 + 3x_1^2x_2^2 + 6x_1^2x_2^2),$$

and substituting for the variables x_i gives

$$r^6 + r^5b + 2r^4b^2 + 3r^3b^3 + 2r^2b^4 + rb^5 + b^6.$$

Recall that the "colors" of the edges in this example are "included" and "excluded". If we set $b = 1$ and $r = i$ (for "included") we get

$$i^6 + i^5 + 2i^4 + 3i^3 + 2i^2 + i + 1,$$

interpreted as one graph with 6 edges, one with 5, two with 4, three with 3, two with 2, one with 1, and one with zero edges, since $1 = i^0$. (Of course, if we are interested in the inventory in the final form, we can skip the step using r and b by substituting $x_j = i^j + 1$ in the cycle index.) □

It is possible, though a bit difficult, to see that for n vertices the cycle index is

$$\mathcal{P}_G = \sum_{\mathbf{j}} \prod_{k=1}^{n} \frac{1}{k^{j_k} j_k!} \prod_{k=1}^{\lfloor n/2 \rfloor} (x_k x_{2k}^{k-1})^{j_{2k}} \prod_{k=1}^{\lfloor (n-1)/2 \rfloor} x_{2k+1}^{kj_{2k+1}} \prod_{k=1}^{\lfloor n/2 \rfloor} x_k^{kC(j_k,2)} \prod_{1 \le r < s \le n-1} x_{\mathrm{lcm}(r,s)}^{\gcd(r,s) j_r j_s},$$

where the sums are over all partitions $\mathbf{j} = (j_1, j_2, \ldots, j_n)$ of n, that is, over all $\mathbf{j}$ such that $j_1 + 2j_2 + 3j_3 + \cdots + nj_n = n$, and $C(m,2) = \binom{m}{2}$. This is where the formula 6.2.1 comes from, substituting $x_i = 2$ for all i.

With this formula and a computer it is easy to compute the inventory of n-vertex graphs when n is not too large. When $n = 5$, the inventory is

$$i^{10} + i^9 + 2i^8 + 4i^7 + 6i^6 + 6i^5 + 6i^4 + 4i^3 + 2i^2 + i + 1.$$

We can use Sage to do the computations involved in finding the cycle index for graphs.

Exercises 6.3.

1. Find the cycle index $\mathcal{P}_G$ for the group of permutations of the vertices of a regular tetrahedron induced by the rigid motions. (See exercise 1 in section 6.2.)
2. Using the previous exercise, write out a full inventory of colorings of the vertices of a regular tetrahedron induced by the rigid motions, with three colors, as in example 6.3.5. You may use Sage or some other computer algebra system.
3. Find the cycle index $\mathcal{P}_G$ for the group of permutations of the edges of K_5. (See exercise 5 in section 6.2. Don't use the general formula above.)
4. Using the previous exercise, write out a full inventory of the graphs on five vertices, as in example 6.3.6. You may use Sage or some other computer algebra system.

A

Hints

1.6.2. Every positive integer can be written as $j \cdot 2^k$, with j odd and $k \geq 0$.

Index