Combinatorics

an upper-level introductory course
in enumeration, graph theory, and design theory

by

Joy Morris
University of Lethbridge

Version 1.1 of June 2017

Please send comments and corrections to:
Joy.Morris@uleth.ca

Contents

Part I. Enumeration

Part II. Graph Theory

Part III. Design Theory

Chapter 1

What is Combinatorics?

Combinatorics is a subfield of “discrete mathematics,” so we should begin by asking what discrete mathematics means. The differences are to some extent a matter of opinion, and various mathematicians might classify specific topics differently.

“Discrete” should not be confused with “discreet,” which is a much more commonly-used word. They share the same Latin root, “discretio,” which has to do with wise discernment or separation. In the mathematical “discrete,” the emphasis is on separateness, so “discrete” is the opposite of “continuous.” If we are studying objects that can be separated and treated as a (generally countable) collection of units rather than a continuous structure, then this study falls into discrete mathematics.

In calculus, we deal with continuous functions, so calculus is not discrete mathematics. In linear algebra, our matrices often have real entries, so linear algebra also does not fall into discrete mathematics.

Text books on discrete mathematics often include some logic, as discrete mathematics is often used as a gateway course for upper-level math. Elementary number theory and set theory are also sometimes covered. Algorithms are a common topic, as algorithmic techniques tend to work very well on the sorts of structures that we study in discrete mathematics.

In Combinatorics, we focus on combinations and arrangements of discrete structures. There are five major branches of combinatorics that we will touch on in this course: enumeration, graph theory, Ramsey Theory, design theory, and coding theory. (The related topic of cryptography can also be studied in combinatorics, but we will not touch on it in this course.) We will focus on enumeration, graph theory, and design theory, but will briefly introduce the other two topics.

1A. Enumeration

Enumeration is a big fancy word for counting. If you’ve taken a course in probability and statistics, you’ve already covered some of the techniques and problems we’ll be covering in this course. When a statistician (or other mathematician) is calculating the “probability” of a particular outcome in circumstances where all outcomes are equally likely, what they usually do is enumerate all possible outcomes, and then figure out how many of these include the outcome they are looking for.

EXAMPLE 1.1. What is the probability of rolling a 3 on a 6-sided die?

SOLUTION. To figure this out, a mathematician would count the sides of the die (there are six) and count how many of those sides display a three (one of them). She would conclude that the probability of rolling a 3 on a 6-sided die is 1/6 (one in six). □

That was an example that you could probably figure out without having studied enumeration or probability, but it nonetheless illustrates the basic principle behind many calculations of probability. The object of enumeration is to enable us to count outcomes in much more complicated situations. This sometimes has natural applications to questions of probability, but our focus will be on the counting, not on the probability.

After studying enumeration in this course, you should be able to solve problems such as:

- If you are playing Texas Hold'em poker against a single opponent, and the two cards in your hand are a pair, what is the probability that your opponent has a higher pair?
- How many distinct Shidokus (4-by-4 Sudokus) are there?
- How many different orders of five items can be made from a bakery that makes three kinds of cookies?
- Male honeybees come from a queen bee's unfertilised eggs, so have only one parent (a female). Female honeybees have two parents (one male, one female). Assuming all ancestors were distinct, how many ancestors does a male honeybee have from 10 generations ago?

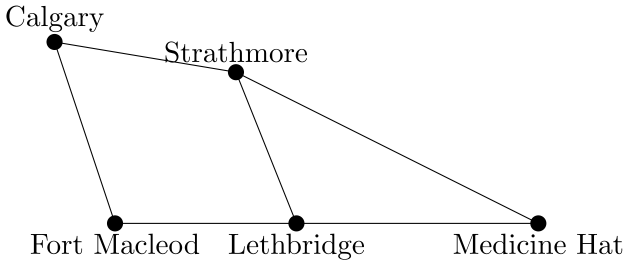
Although all of these questions (and many others that arise naturally) may be of interest to you, the reason we begin our study with enumeration is because we'll be able to use many of the techniques we learn, to count the other structures we'll be studying.

1B. Graph Theory

When a mathematician talks about graph theory, she is not referring to the "graphs" that you learn about in school, that can be produced by a spreadsheet or a graphing calculator. The "graphs" that are studied in graph theory are models of networks.

Any network can be modeled by using dots to represent the nodes of the network (the cities, computers, cell phones, or whatever is being connected) together with lines to represent the connections between those nodes (the roads, wires, wireless connections, etc.). This model is called a graph. It is important to be aware that only at a node may information, traffic, etc. may pass from one edge of a graph to another edge. If we want to model a highway network using a graph, and two highways intersect in the middle of nowhere, we must still place a node at that intersection. If we draw a graph in which edges cross over each other but there is no node at that point, you should think of it as if there is an overpass there with no exits from one highway to the other: the roads happen to cross, but they are not connecting in any meaningful sense.

EXAMPLE 1.2. The following diagram:



is a graph.

Many questions that have important real-world applications can be modeled with graphs. These are not always limited to questions that seem to apply to networks. Some questions can be modeled as graphs by using lines to represent constraints or some other relationship between them (e.g. the nodes might represent classes, with a line between them if they cannot be scheduled at the same time, or some nodes might represent students and others classes, with a line between a student and each of the classes he or she is taking).

After studying graph theory in this course, you should be able to solve problems such as:

- How can we find a good route for garbage trucks to take through a particular city?
- Is there a delivery route that visits every city in a particular area, without repetition?
- Given a collection of project topics and a group of students each of whom has expressed interest in some of the topics, is it possible to assign each student a unique topic that interests him or her?
- A city has bus routes all of which begin and end at the bus terminal, but with different schedules, some of which overlap. What is the least number of buses (and drivers) required in order to be able to complete all of the routes according to the schedule?
- Create a schedule for a round-robin tournament that uses as few time slots as possible.

Some of these questions you may only be able to answer for particular kinds of graphs.

Graph theory is a relatively "young" branch of mathematics. Although some of the problems and ideas that we will study date back a few hundred years, it was not until the 1930s that these individual problems were gathered together and a unified study of the theory of graphs began to develop.

1C. Ramsey Theory

Ramsey theory takes its name from Frank P. Ramsey, a British mathematician who died in 1930 at the tragically young age of 26, when he developed jaundice after an operation.

Ramsey was a logician. A result that he considered a minor lemma in one of his logic papers now bears the name "Ramsey's Theorem" and was the basis for this branch of mathematics. Its statement requires a bit of graph theory: given c colours and fixed sizes $n_1, \ldots, n_c$, there is an integer $r = R(n_1, \ldots, n_c)$ such that for any colouring the edges of of a complete graph on r vertices, there must be some i between 1 and c such that there is a complete subgraph on n_i vertices, all of whose edges are coloured with colour i.

In addition to requiring some graph theory, that statement was a bit technical. In much less precise terms that don't require so much background knowledge (but could be misleading in specific situations), Ramsey Theory asserts that if structure is big enough and contains a property we are interested in, then no matter how we cut it into pieces, at least one of the pieces should also have that property. One major theorem in Ramsey Theory is van der Waerden's Theorem, which states that for any two constants c and n, there is a constant $V(c, n)$ such that if we take $V(c, n)$ consecutive numbers and colour them with c colours, there must be an arithmetic progression of length n all of whose members have been coloured with the same colour.

EXAMPLE 1.3. Here is a small example of van der Waerden's Theorem. With two colours and a desired length of 3 for the arithmetic progression, we can show that $V(2, 3) > 8$ using the following colouring:

3 4 5 6 7 8 9 10

(In case it is difficult to see, we point out that 3, 4, 7, and 8 are black, while 5, 6, 9, and 10 are grey, a different colour.) Notice that with eight consecutive integers, the difference in a three-term arithmetic progression cannot be larger than three. For every three-term arithmetic progression with difference of one, two, or three, it is straightforward to check that the numbers have not all received the same colour.

In fact, $V(2, 3) = 9$, but proving this requires exhaustive testing.

We will touch lightly on Ramsey Theory in this course, specifically on Ramsey's Theorem itself, in the context of graph theory.

1D. Design Theory

Like graph theory, design theory is probably not what any non-mathematician might expect from its name.

When researchers conduct an experiment, errors can be introduced by many factors (including, for example, the timing or the subject of the experiment). It is therefore important to replicate the experiment a number of times, to ensure that these unintended variations do not account for the success of a particular treatment. If a number of different treatments are being tested, replicating all of them numerous times becomes costly and potentially infeasible. One way to reduce the total number of trials while still maintaining the accuracy, is to test multiple treatments on each subject, in different combinations.

One of the major early motivations for design theory was this context: given a fixed number of total treatments, and a fixed number of treatments we are willing to give to any subject, can we find combinations of the possible treatments so that each treatment is given to some fixed number of subjects, and any pair of treatments is given together some fixed number of times (often just once). This is the basic structure of a block design.

EXAMPLE 1.4. Suppose that we have seven different fertilisers and seven garden plots on which to try them. We can organise them so that each fertiliser is applied to three of the plots, each garden plot receives 3 fertilisers, and any pair of fertilisers is used together on precisely one of the plots. If the different fertilisers are numbered one through seven, then a method for arranging them is to place fertilisers 1, 2, and 3 on the first plot; 1, 4, and 5 on the second; 1, 6, and 7 on the third; 2, 4, and 6 on the fourth; 2, 5, and 7 on the fifth; 3, 4, and 7 on the sixth; and 3, 5, and 6 on the last. Thus,

$$\begin{array}{ccc} 123 & 145 & 167 \\ 246 & 257 & 347 \\ & 356 & \end{array}$$

is a design.

This basic idea can be generalised in many ways, and the study of structures like these is the basis of design theory. In this course, we will learn some facts about when designs exist, and how to construct them.

After studying design theory in this course, you should be able to solve problems such as:

Is it possible for a design to exist with a particular set of parameters?

What methods might we use in trying to construct a design?

1E. Coding Theory

In many people's minds "codes" and "cryptography" are inextricably linked, and they might be hard-pressed to tell you the difference. Nonetheless, the two topics are vastly different, as is the mathematics involved in them.

Coding theory is the study of encoding information into different symbols. When someone uses a code in an attempt to make a message that only certain other people can read, this becomes cryptography. Cryptographers study strategies for ensuring that a code is difficult to "break" for those who don't have some additional information. In coding theory, we ignore the question of who has access to the code and how secret it may be. Instead, one of the primary concerns becomes our ability to detect and correct errors in the code.

Codes are used for many purposes in which the information is not intended to be secret. For example, computer programs are transformed into long strings of binary data, that a computer reinterprets as instructions. When you text a photo to a friend, the pixel and colour information are converted into binary data to be transmitted through radio waves. When you listen to an .mp3 file, the sound frequencies of the music have been converted into binary data that your computer decodes back into sound frequencies.

Electronic encoding is always subject to interference, which can cause errors. Even when a coded message is physically etched onto a device (such as a dvd), scratches can make some parts of the code illegible. People don't like it when their movies, music, or apps freeze, crash, or skip over something. To avoid this problem, engineers use codes that allow our devices to automatically detect, and correct, minor errors that may be introduced.

In coding theory, we learn how to create codes that allow for error detection and correction, without requiring excessive memory or storage capacity. Although coding theory is not a focus of this course, designs can be used to create good codes. We will learn how to make codes from designs, and what makes these codes "good."

EXAMPLE 1.5. Suppose we have a string of binary information, and we want the computer to store it so we can detect if an error has arisen. There are two symbols we need to encode: 0 and 1. If we just use 0 for 0 and 1 for 1, we'll never know if a bit has been flipped (from 0 to 1 or vice versa). If we use 00 for 0 and 01 for 1, then if the first bit gets flipped we'll know there was an error (because the first bit should never be 1), but we won't notice if the second was flipped. If we use 00 for 0 and 11 for 1, then we will be able to detect an error, as long as at most one bit gets flipped, because flipping one bit of either code word will result in either 01 or 10, neither of which is a valid code word. Thus, this code allows us to detect an error. It does not allow us to correct an error, because even knowing that a single bit has been flipped, there is no way of knowing whether a 10 arose from a 00 with the first bit flipped, or from a 11 with the second bit flipped. We would need a longer code to be able to correct errors.

After our study of coding theory, you should be able to solve problems such as:

- Given a code, how many errors can be detected?
- Given a code, how many errors can be corrected?
- Construct some small codes that allow detection and correction of small numbers of errors.

EXERCISES 1.6. Can you come up with an interesting counting problem that you wouldn't know how to solve?

SUMMARY:

- enumeration
- graph theory
- Ramsey theory
- design theory
- coding theory

Part I

Enumeration

Chapter 2

Basic Counting Techniques

When we are trying to count the number of ways in which something can happen, sometimes the answer is very obvious. For example, if a doughnut shop has five different kinds of doughnuts for sale and you are planning to buy one doughnut, then you have five choices.

There are some ways in which the situation can become slightly more complicated. For example, perhaps you haven't decided whether you'll buy a doughnut or a bagel, and the store also sells three kinds of bagels. Or perhaps you want a cup of coffee to go with your doughnut, and there are four different kinds of coffee, each of which comes in three different sizes.

These particular examples are fairly small and straightforward, and you could list all of the possible options if you wished. The goal of this chapter is to use simple examples like these to demonstrate two rules that allow us to count the outcomes not only in these situations, but in much more complicated circumstances. These rules are the *product rule*, and the *sum rule*.

2A. The product rule

The product rule is a rule that applies when we there is more than one variable (i.e. thing that can change) involved in determining the final outcome.

EXAMPLE 2.1. Consider the example of buying coffee at a coffee shop that sells four varieties and three sizes. When you are choosing your coffee, you need to choose both variety and size. One way of figuring out how many choices you have in total, would be to make a table. You could label the columns with the sizes, and the rows with the varieties (or vice versa, it doesn't matter). Each entry in your table will be a different combination of variety and size:

	Small	**Medium**	**Large**
Latte	small latte	medium latte	large latte
Mocha	small mocha	medium mocha	large mocha
Espresso	small espresso	medium espresso	large espresso
Cappuccino	small cappuccino	medium cappuccino	large cappuccino

As you can see, a different combination of variety and size appears in each space of the table, and every possible combination of variety and size appears somewhere. Thus the total number of possible choices is the number of entries in this table. Although in a small example like this we could simply count all of the entries and see that there are twelve, it will be more useful to notice that elementary arithmetic tells us that the number of entries in the table will be the number of rows times the number of columns, which is four times three.

In other words, to determine the total number of choices you have, we multiply the number of choices of variety (that is, the number of rows in our table) by the number of choices of size (that is, the number of columns in our table). This is an example of what we'll call the *product rule.*

We're now ready to state the product rule in its full generality.

THEOREM 2.2. Product Rule *Suppose that when you are determining the total number of outcomes, you can identify two different aspects that can vary. If there are n_1 possible outcomes for the first aspect, and for each of those possible outcomes, there are n_2 possible outcomes for the second aspect, then the total number of possible outcomes will be $n_1 n_2$.*

In the above example, we can think of the aspects that can change as being the variety of coffee, and the size. There are four outcomes (choices) for the first aspect, and three outcomes (choices) for the second aspect, so the total number of possible outcomes is $4 \cdot 3 = 12$.

Sometimes it seems clear that there are more than two aspects that are varying. If this happens, we can apply the product rule more than once to determine the answer, by first identifying two aspects (one of which may be "all the rest"), and then subdividing one or both of those aspects. An example of this is the problem posed earlier of buying a doughnut to go with your coffee.

EXAMPLE 2.3. Kyle wants to buy coffee and a doughnut. The local doughnut shop has five kinds of doughnuts for sale, and sells four varieties of coffee in three sizes (as in Example 2.1). How many different orders could Kyle make?

SOLUTION. A natural way to divide Kyle's options into two aspects that can vary, is to consider separately his choice of doughnut, and his choice of coffee. There are five choices for the kind of doughnut he orders, so $n_1 = 5$. For choosing the coffee, we have already used the product rule in Example 2.1 to determine that the number of coffee options is $n_2 = 12$.

Thus the total number of different orders Kyle could make is $n_1 n_2 = 5 \cdot 12 = 60$. □

Let's go through an example that more clearly involves repeated applications of the product rule.

EXAMPLE 2.4. Chloë wants to manufacture children's t-shirts. There are generally three sizes of t-shirts for children: small, medium, and large. She wants to offer the t-shirts in eight different colours (blue, yellow, pink, green, purple, orange, white, and black). The shirts can have an image on the front, and a slogan on the back. She has come up with three images, and five slogans.

To stock her show room, Chloë wants to produce a single sample of each kind of shirt that she will be offering for sale. The shirts cost her \$4 each to produce. How much are the samples going to cost her (in total)?

SOLUTION. To solve this problem, observe that to determine how many sample shirts Chloë will produce, we can consider the size as one aspect, and the style (including colour, image, and slogan) as the other. There are $n_1 = 3$ sizes. So the number of samples will be three times n_2, where n_2 is the number of possible styles.

We now break n_2 down further: to determine how many possible styles are available, you can divide this into two aspects: the colour, and the decoration (image and slogan). There are $n_{2,1} = 8$ colours. So the number of styles will be eight times $n_{2,2}$, where $n_{2,2}$ is the number of possible decorations (combinations of image and slogan) that are available.

We can break $n_{2,2}$ down further: to determine how many possible decorations are available, you divide this into the two aspects of image and slogan. There are $n_{2,2,1} = 3$ possible images, and $n_{2,2,2} = 5$ possible slogans, so the product rule tells us that there are $n_{2,2} = 3 \cdot 5 = 15$ possible combinations of image and slogan (decorations).

Putting all of this together, we see that Chloë will have to create $3(8(3 \cdot 5)) = 360$ sample t-shirts. As each one costs \$4, her total cost will be \$1440. □

Notice that finding exactly two aspects that vary can be quite artificial. Example 2.4 serves as a good demonstration for a generalisation of the product rule as we stated it above. In that example, it would have been more natural to have considered from the start that there were four apparent aspects to the t-shirts that can vary: size; colour; image; and slogan. The total number of t-shirts she needed to produce was the product of the number of possible outcomes of each of these aspects: $3 \cdot 8 \cdot 3 \cdot 5 = 360$.

THEOREM 2.5. Product Rule for many aspects *Suppose that when you are determining the total number of outcomes, you can identify k different aspects that can vary. If for each i between 1 and k there are n_i possible outcomes for the ith aspect, then the total number of possible outcomes will be $\prod_{i=1}^{k} n_i$ (that is, the product as i goes from 1 to k of the n_i).*

Now let's look at an example where we are trying to evaluate a probability. Since this course is about counting rather than probability, we'll restrict our attention to examples where all outcomes are equally likely. Under this assumption, in order to determine a probability, we can count the number of outcomes that have the property we're looking for, and divide by the total number of outcomes.

EXAMPLE 2.6. Peter and Mary have two daughters. What is the probability that their next two children will also be girls?

SOLUTION. To answer this, we consider each child as a different aspect. There are two possible sexes for their third child: boy or girl. For each of these, there are two possible choices for their fourth child: boy or girl. So in total, the product rule tells us that there are $2 \cdot 2 = 4$ possible combinations for the sexes of their third and fourth children. This will be the denominator of the probability.

To determine the numerator (that is, the number of ways in which both children can be girls), we again consider each child as a different aspect. There is only one possible way for the third child to be a girl, and then there is only one possible way for the fourth child to be a girl. So in total, only one of the four possible combinations of sexes involves both children being girls.

The probability that their next two children will also be girls is 1/4. □

Notice that in this example, the fact that Peter and Mary's first two children were girls was irrelevant to our calculations, because it was already a known outcome, over and done with, so is true no matter what may happen with their later children. If Peter and Mary hadn't yet had any children and we asked for the probability that their first four children will all be girls, then our calculations would have to include both possible options for the sex of each of their first two children. In this case, the final probability would be 1/16 (there are 16 possible combinations for the sexes of four children, only one of which involves all four being female).

EXERCISES 2.7. Use only the product rule to answer the following questions:

1) The car Jack wants to buy comes in four colours; with or without air conditioning; with five different options for stereo systems; and a choice of none, two, or four floor mats. If the dealership he visits has three cars in the lot, each with different options, what is the probability that one of the cars they have in stock has exactly the options he wants?

2) Candyce is writing a "Choose your own adventure" book in which she wants every possible choice to result in a different ending. If there are four points at which choices

must be made in every storyline, and there are three choices the first time but two every time after that, how many endings does Candyce need to write?

3) William is buying five books. For each book he has a choice of version: hardcover, paperback, or electronic. In how many different ways can he make his selection?

2B. The sum rule

The sum rule is a rule that can be applied to determine the number of possible outcomes when there are two different things that you might choose to do (and various ways in which you can do each of them), and you cannot do both of them. Often, it is applied when there is a natural way of breaking the outcomes down into cases.

EXAMPLE 2.8. Recall the example of buying a bagel *or* a doughnut at a doughnut shop that sells five kinds of doughnuts and three kinds of bagels. You are only choosing one or the other, so one way to determine how many choices you have in total, would be to write down all of the possible kinds of doughnut in one list, and all of the possible kinds of bagel in another list:

Doughnuts	**Bagels**
chocolate glazed	blueberry
chocolate iced	cinnamon raisin
honey cruller	plain
custard filled	
original glazed	

The total number of possible choices is the number of entries that appear in the two lists combined, which is five plus three.

In other words, to determine the number of choices you have, we add the number of choices of doughnut (that is, the number of entries in the first list) and the number of choices of bagel (that is, the number of entries in the second list). This is an example of the *sum rule.*

We're now ready to state the sum rule in its full generality.

THEOREM 2.9. Sum Rule *Suppose that when you are determining the total number of outcomes, you can identify two distinct cases with the property that every possible outcome lies in exactly one of the cases. If there are n_1 possible outcomes in the first case, and n_2 possible outcomes in the second case, then the total number of possible outcomes will be $n_1 + n_2$.*

It's hard to do much with the sum rule by itself, but we'll cover a couple more examples and then in the next section, we'll get into some more challenging examples where we combine the two rules.

Sometimes the problem naturally splits into more than two cases, with every possible outcome lying in exactly one of the cases. If this happens, we can apply the sum rule more than once to determine the answer. First we identify two cases (one of which may be "everything else"), and then subdivide one or both of the cases. Let's look at an example of this.

EXAMPLE 2.10. Mary and Peter are planning to have no more than three children. What are the possible combinations of girls and boys they might end up with, if we aren't keeping track of the order of the children? (By not keeping track of the order of the children, I mean that we'll consider having two girls followed by one boy as being the same as having two girls and one boy in any other order.)

SOLUTION. To answer this question, we'll break the problem into cases. First we'll divide the problem into two possibilities: Mary and Peter have no children; or they have at least one child. If Mary and Peter have no children, this can happen in only one way (no boys and no girls). If

Mary and Peter have at least one child, then they have between one and three children. We'll have to break this down further to find how many outcomes are involved.

We break the case where Mary and Peter have between one and three children down into two cases: they might have one child, or they might have more than one child. If they have one child, that child might be a boy or a girl, so there are two possible outcomes. If they have more than one child, again we'll need to further subdivide this case.

The case where Mary and Peter have either two or three children naturally breaks down into two cases: they might have two children, or they might have three children. If they have two children, the number of girls they have might be zero, one, or two, so there are three possible outcomes (the remaining children, if any, must all be boys). If they have three children, the number of girls they have might be zero, one, two, or three, so there are four possible outcomes (again, any remaining children must be boys).

Now we put all of these outcomes together with the sum rule. We conclude that in total, there are $1 + (2 + (3 + 4)) = 10$ different combinations of girls and boys that Mary and Peter might end up with. □

Notice that it was artificial to repeatedly break this example up into two cases at a time. Thus, Example 2.10 serves as a good demonstration for a generalisation of the sum rule as we stated it above. It would have been more natural to have broken the problem of Mary and Peter's kids up into four cases from the beginning, depending on whether they end up with zero, one, two, or three kids. The total number of combinations of girls and boys that Mary and Peter might end up with, is the sum of the combinations they can end up with in each of these cases; that is, $1 + 2 + 3 + 4 = 10$.

THEOREM 2.11. Sum Rule for many cases *Suppose that when you are determining the total number of outcomes, you can identify k distinct cases with the property that every possible outcome lies in exactly one of the cases. If for each i between 1 and k there are n_i possible outcomes in the ith case, then the total number of possible outcomes will be $\sum_{i=1}^{k} n_i$ (that is, the sum as i goes from 1 to k of the n_i).*

There is one other important way to use the sum rule. This application is a bit more subtle. Suppose you know the total number of outcomes, and you want to know the number of outcomes that *don't* include a particular event. The sum rule tells us that the total number of outcomes is comprised of the outcomes that *do* include that event, together with the ones that don't. So if it's easy to figure out how many outcomes include the event that interests you, then you can subtract that from the total number of outcomes to determine how many outcomes *exclude* that event. Here's an example.

EXAMPLE 2.12. There are 216 different possible outcomes from rolling a white die, a red die, and a yellow die. (You can work this out using the product rule.) How many of these outcomes involve rolling a one on two or fewer of the dice?

SOLUTION. Tackling this problem directly, you might be inclined to split it into three cases: outcomes that involve rolling no ones, those that involve rolling exactly one one, and those that involve rolling exactly two ones. If you try this, the analysis will be long and fairly involved, and will include both the product rule and the sum rule. If you are careful, you will be able to find the correct answer this way.

We'll use a different approach, by first counting the outcomes that we *don't* want: those that involve getting a one on all three of the dice. There is only one way for this to happen: all three of the dice have to roll ones! So the number of outcomes that involve rolling ones on two or fewer of the dice, will be $216 - 1 = 215$. □

EXERCISES 2.13. Use only the sum rule to answer the following questions:

1) I have four markers on my desk: one blue and three black. Every day on my way to class, I grab three of the markers without looking. There are four different markers that could be left behind, so there are four combinations of markers that I could take with me. What is the probability that I take the blue marker?
2) Maple is thinking of either a letter, or a digit. How many different things could she be thinking of?
3) How many of the 16 four-bit binary numbers have at most one 1 in them?

2C. Putting them together

When we combine the product rule and the sum rule, we can explore more challenging questions.

EXAMPLE 2.14. Grace is staying at a bed-and-breakfast. In the evening, she is offered a choice of menu items for breakfast in bed, to be delivered the next morning. There are three kinds of items: main dishes, side dishes, and beverages. She is allowed to choose up to one of each, but some of them come with optional extras. From the menu below, how many different breakfasts could she order?

Menu

Mains	Sides	Beverages
pancakes	fruit cup	coffee
oatmeal	toast	tea
omelette		orange juice
waffles		

Pancakes, waffles, and toast come with butter.
Coffee and tea come with milk and sugar.

Optional extras:
marmalade, lemon curd, or blackberry jam for toast;
maple syrup for pancakes or waffles.

SOLUTION. We see that the number of choices Grace has available depends partly on whether or not she orders an item or items that include optional extras. We will therefore divide our consideration into four cases:

1) Grace does not order any pancakes, waffles, or toast.
2) Grace orders pancakes or waffles, but does not order toast.
3) Grace does not order pancakes or waffles, but does order toast.
4) Grace orders toast, and also orders either pancakes or waffles.

In the first case, Grace has three possible choices for her main dish (oatmeal, omelette, or nothing). For each of these, she has two choices for her side dish (fruit cup, or nothing). For each of these, she has four choices for her beverage (coffee, tea, orange juice, or nothing). Using the product rule, we conclude that Grace could order $3 \cdot 2 \cdot 4 = 24$ different breakfasts that do not include pancakes, waffles, or toast.

In the second case, Grace has two possible choices for her main dish (pancakes, or waffles). For each of these, she has two choices for her side dish (fruit cup, or nothing). For each of these, she has four choices for her beverage. In addition, for each of her choices of pancakes or waffles, she can choose to have maple syrup, or not (two choices). Using the product rule, we conclude that Grace could order $2 \cdot 2 \cdot 4 \cdot 2 = 32$ different breakfasts that include pancakes or waffles, but not toast.

In the third case, Grace has three possible choices for her main dish (oatmeal, omelette, or nothing). For each of these, she has only one possible side dish (toast), but she has four choices for what to put on her toast (marmalade, lemon curd, blackberry jam, or nothing). For each of these choices, she has four choices of beverage. Using the product rule, we conclude that Grace could order $3 \cdot 4 \cdot 4 = 48$ different breakfasts that include toast, but do not include pancakes or waffles.

In the final case, Grace has two possible choices for her main dish (pancakes, or waffles). She has two choices for what to put on her main dish (maple syrup, or only butter). She is having toast, but has four choices for what to put on her toast. Finally, she again has four choices of beverage. Using the product rule, we conclude that Grace could order $2 \cdot 2 \cdot 4 \cdot 4 = 64$ different breakfasts that include toast as well as either pancakes or waffles.

Using the sum rule, we see that the total number of different breakfasts Grace could order is $24 + 32 + 48 + 64 = 168$. □

Here's another example of combining the two rules.

EXAMPLE 2.15. The types of license plates in Alberta that are available to individuals (not corporations or farms) for their cars or motorcycles, fall into one of the following categories:

- vanity plates;
- regular car plates;
- veteran plates; or
- motorcycle plates.

None of these license plates use the letters I or O.

Regular car plates have one of two formats: three letters followed by three digits; or three letters followed by four digits (in the latter case, none of the letters A, E, I, O, U, or Y is used).

Veteran plates begin with the letter V, followed by two other letters and two digits. Motorcycle plates have two letters followed by three digits.

Setting aside vanity plates and ignoring the fact that some three-letter words are avoided, how many license plates are available to individuals in Alberta for their cars or motorcycles?

SOLUTION. To answer this question, there is a natural division into four cases: regular car plates with three digits; regular car plates with four digits; veteran plates; and motorcycle plates.

For a regular car plate with three digits, there are 24 choices for the first letter, followed by 24 choices for the second letter, and 24 choices for the third letter. There are 10 choices for the first digit, 10 choices for the second digit, and 10 choices for the third digit. Using the product rule, the total number of license plates in this category is $24^3 \cdot 10^3 = 13,824,000$.

For a regular car plate with four digits, there are 20 choices for the first letter, followed by 20 choices for the second letter, and 20 choices for the third letter. There are 10 choices for the first digit, 10 choices for the second digit, 10 choices for the third digit, and 10 choices for the fourth digit. Using the product rule, the total number of license plates in this category is $20^3 \cdot 10^4 = 80,000,000$.

For a veteran plate, there are 24 choices for the first letter, followed by 24 choices for the second letter. There are 10 choices for the first digit, and 10 choices for the second digit. Using the product rule, the total number of license plates in this category is $24^2 \cdot 10^2 = 57,600$.

Finally, for a motorcycle plate, there are 24 choices for the first letter, followed by 24 choices for the second letter. There are 10 choices for the first digit, 10 choices for the second digit, and 10 choices for the third digit. Using the product rule, the total number of license plates in this category is $24^2 \cdot 10^3 = 576,000$.

Using the sum rule, we see that the total number of license plates is

$$13,824,000 + 80,000,000 + 57,600 + 576,000$$

which is $94,457,600$. □

It doesn't always happen that the sum rule is applied first to break the problem down into cases, followed by the product rule within each case. In some problems, these might occur in the other order. Sometimes there may seem to be one "obvious" way to look at the problem, but often there is more than one equally effective analysis, and different analyses might begin with different rules.

In Example 2.14, we could have begun by noticing that no matter what else she may choose, Grace has four possible options for her beverage. Thus, the total number of possible breakfast orders will be four times the number of possible orders of main and side (with optional extras). Then we could have proceeded to analyse the number of possible choices for her main dish and her side dish (together with the extras). Breaking down the choices for her main and side dishes into the same cases as before, we could see that there are $3 \cdot 2 = 6$ choices in the first case; $2 \cdot 2 \cdot 2 = 8$ choices in the second case; $3 \cdot 4 = 12$ choices in the third case; and $2 \cdot 2 \cdot 4 = 16$ choices in the fourth case. Thus she has a total of $6 + 8 + 12 + 16 = 42$ choices for her main and side dishes. The product rule now tells us that she has $4 \cdot 42 = 168$ possible orders for her breakfast.

Let's run through one more (simpler) example of using both the sum and product rules, and work out the answer in two different ways.

EXAMPLE 2.16. Kathy plans to buy her Dad a shirt for his birthday. The store she goes to has three different colours of short-sleeved shirts, and six different colours of long-sleeved shirts. They will gift-wrap in her choice of two wrapping papers. Assuming that she wants the shirt gift-wrapped, how many different options does she have for her gift?

SOLUTION. Let's start by applying the product rule first. There are two aspects that she can vary: the shirt, and the wrapping. She has two choices for the wrapping, so her total number of options will be twice the number of shirt choices that she has. For the shirt, we break her choices down into two cases: if she opts for a short-sleeved shirt then she has three choices (of colour), while if she opts for a long-sleeved shirt then she has six choices. In total she has $3 + 6 = 9$ choices for the shirt. Using the product rule, we see that she has $2 \cdot 9 = 18$ options for her gift.

Alternatively, we could apply the sum rule first. We will consider the two cases: that she buys a short-sleeved shirt; or a long-sleeved shirt. If she buys a short-sleeved shirt, then she has three options for the shirt, and for each of these she has two options for the wrapping, making (by the product rule) $3 \cdot 2 = 6$ options of short-sleeved shirts. If she buys a long-sleeved shirt, then she has six options for the shirt, and for each of these she has two options for the wrapping, making (by the product rule) $6 \cdot 2 = 12$ options of long-sleeved shirts. Using the sum rule, we see that she has $6 + 12 = 18$ options for her gift. □

EXERCISES 2.17. How many passwords can be created with the following constraints:

1) The password is three characters long and contains two lowercase letters and one digit, in some order.
2) The password is eight or nine characters long and consists entirely of digits.
3) The password is five characters long and consists of lowercase letters and digits. All of the letters must come before all of the digits in the password, but there can be any number of letters (from zero through five).

4) The password is four characters long and consists of two characters that can be either digits or one of 16 special characters, and two lowercase letters. The two letters can be in any two of the four positions.

5) The password is eight characters long and must include at least one letter and at least one digit.

6) The password is eight characters long and cannot include any character more than once.

EXERCISES 2.18.

1) There are 8 buses a day from Toronto to Ottawa, 20 from Ottawa to Montreal, and 9 buses directly from Toronto to Montreal. Assuming that you do not have to complete the trip in one day (so the departure and arrival times of the buses is not an issue), how many different schedules could you use in travelling by bus from Toronto to Montreal?

2) How many 7-bit ternary strings (that is, strings whose only entries are 0, 1, or 2) begin with either 1 or 01?

2D. Summing up

Very likely you've used the sum rule or the product rule when counting simple things, without even stopping to think about what you were doing. The reason we're going through each of them very slowly and carefully, is because whsen we start looking at more complicated problems, our uses of the sum and product rules will become more subtle. If we don't have a very clear understanding in very simple situations of what we are doing and why, we'll be completely lost when we get to more difficult examples.

It's dangerous to try to come up with a simple guideline for when to use the product rule and when to use the sum rule, because such a guideline will often go wrong in complicated situations. Nonetheless, a good question to ask yourself when you are trying to decide which rule to use is, "Would I describe this with the word 'and,' or the word 'or'?" The word "and" is generally used in situations where it's appropriate to use the product rule, while "or" tends to go along with the sum rule.

Let's see how this applies to each of the examples we've looked at in this chapter.

In Example 2.1, you needed to choose the size *and* the variety for your coffee. In Example 2.3, Kyle wanted to choose a doughnut *and* coffee. In Example 2.4, Chloë needed to determine the size *and* the colour *and* the image *and* the slogan for each t-shirt. In Example 2.6, we wanted to know the sex of Peter and Mary's third *and* fourth children. So in each of these examples, we used the product rule.

In Example 2.8, you needed to choose a bagel *or* a doughnut. In Example 2.10, Mary and Peter could have zero *or* one *or* two *or* three children. So in each of these examples, we used the sum rule.

You definitely have to be careful in applying this guideline, as problems can be phrased in a misleading way. We could have said that in Example 2.8, we want to know how many different kinds of doughnuts *and* of bagels there are, altogether. The important point is that you aren't choosing both of these things, though; you are choosing just one thing, and it will be either a doughnut, *or* a bagel.

In Example 2.14, Grace was choosing a main dish *and* a side dish *and* a beverage, so we used the product rule to put these aspects together. Whether or not she had extra options available for her main dish depended on whether she chose pancakes *or* waffles *or* oatmeal *or* omelette *or* nothing, so the sum rule applied here. (Note that we didn't actually consider each of these four things separately, since they naturally fell into two categories. However, we would have reached the same answer if we had considered each of them separately.) Similarly, whether or not she had extra options available for her side dish depended on whether she chose toast *or* not, so again the sum rule applied.

In Example 2.15, the plates can be regular (in either of two ways) *or* veteran *or* motorcycle plates, so the sum rule was used. In each of these categories, we had to consider the options for the first character *and* the second character (and so on), so the product rule applied.

Finally, in Example 2.16, the shirt Kathy chooses can be short-sleeved *or* long-sleeved, so the sum rule applies to that distinction. Since she wants to choose a shirt *and* gift wrap, the product rule applies to that combination.

EXERCISES 2.19. For each of the following problems, do you need to use the sum rule, the product rule, or both?

1) Count all of the numbers that have exactly two digits, and the numbers that have exactly four digits.
2) How many possible outcomes are there from rolling a red die and a yellow die?
3) How many possible outcomes are there from rolling three dice, if you only count the outcomes that involve at most one of the dice coming up as a one?

SUMMARY:

- Product rule.
- Sum rule.
- Combining the product and sum rules.

Chapter 3

Permutations, Combinations, and the Binomial Theorem

The examples we looked at in Chapter 2 involved drawing things from an effectively infinite population – they couldn't run out. When you are making up a password, there is no way you're going to "use up" the letter b by including it several times in your password. In Example 2.4, Chloë's suppliers weren't going to run out of blue t-shirts after printing some of her order, and be unable to complete the remaining blue t-shirts she'd requested. The fact that someone has already had one daughter doesn't mean they've used up their supply of X chromosomes so won't have another daughter.

In this chapter, we'll look at situations where we are choosing more than one item from a finite population in which every item is uniquely identified – for example, choosing people from a family, or cards from a deck.

3A. Permutations

We begin by looking at permutations, because these are a straightforward application of the product rule. The word "permutation" means a rearrangement, and this is exactly what a permutation is: an ordering of a number of distinct items in a line. Sometimes even though we have a large number of distinct items, we want to single out a smaller number and arrange those into a line; this is also a sort of permutation.

DEFINITION 3.1. A **permutation** of n distinct objects is an arrangement of those objects into an ordered line. If $1 \le r \le n$ (and r is a natural number) then an ***r*-permutation** of n objects is an arrangement of r of the n objects into an ordered line.

So a permutation involves choosing items from a finite population in which every item is uniquely identified, and keeping track of the order in which the items were chosen.

Since we are studying enumeration, it shouldn't surprise you that what we'll be asking in this situation is *how many* permutations there are, in a variety of circumstances. Let's begin with an example in which we'll calculate the number of 3-permutations of ten objects (or in this case, people).

EXAMPLE 3.2. Ten athletes are competing for Olympic medals in women's speed skating (1000 metres). In how many ways might the medals end up being awarded?

SOLUTION. There are three medals: gold, silver, and bronze, so this question amounts to finding the number of 3-permutations of the ten athletes (the first person in the 3-permutation is the one who gets the gold medal, the second gets the silver, and the third gets the bronze).

To solve this question, we'll apply the product rule, where the aspects that can vary are the winners of the gold, silver, and bronze medals. We begin by considering how many different athletes might get the gold medal. The answer is that any of the ten athletes might get that medal. No matter which of the athletes gets the gold medal, once that is decided we move our consideration to the silver medal. Since one of the athletes has already been awarded the gold medal, only nine of them remain in contention for the silver medal, so for any choice of athlete who wins gold, the number of choices for who gets the silver medal is nine. Finally, with the gold and silver medalists out of contention for the bronze, there remain eight choices for who might win that medal. Thus, the total number of ways in which the medals might be awarded is $10 \cdot 9 \cdot 8 = 720$. □

We can use the same reasoning to determine a general formula for the number of r-permutations of n objects:

THEOREM 3.3. *The number of r-permutations of n objects is $n(n-1)\dots(n-r+1)$.*

PROOF. There are n ways in which the first object can be chosen (any of the n objects). For each of these possible choices, there remain $n-1$ objects to choose for the second object, etc.□

It will be very handy to have a short form for the number of permutations of n objects.

NOTATION 3.4. We use $n!$ to denote the number of permutations of n objects, so

$$n! = n(n-1)\dots 1.$$

By convention, we define $0! = 1$.

DEFINITION 3.5. We read $n!$ as "***n* factorial**," so n factorial is $n(n-1)\dots 1$.

Thus, the number of r-permutations of n objects can be re-written as $n!/(n-r)!$. When $n = r$ this gives $n!/0! = n!$, making sense of our definition that $0! = 1$.

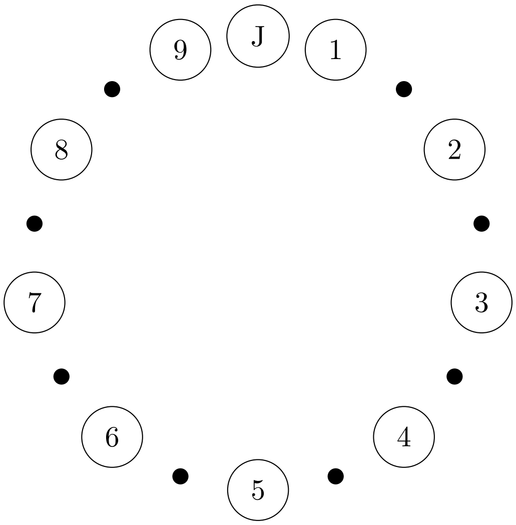
EXAMPLE 3.6. There are 36 people at a workshop. They are seated at six round tables of six people each for lunch. The Morris family (of three) has asked to be seated together (side-by-side). How many different seating arrangements are possible at the Morris family's table?

SOLUTION. First, there are $3! = 6$ ways of arranging the order in which the three members of the Morris family sit at the table. Since the tables are round, it doesn't matter which specific seats they take, only the order in which they sit matters. Once the Morris family is seated, the three remaining chairs are uniquely determined by their positions relative to the Morris family (one to their right, one to their left, and one across from them). There are 33 other people at the conference; we need to choose three of these people and place them in order into the three vacant chairs. There are $33!/(33-3)! = 33!/30!$ ways of doing this. In total, there are $6(33!/30!) = 196,416$ different seating arrangements possible at the Morris family's table. □

By adjusting the details of the preceding example, it can require some quite different thought processes to find the answer.

EXAMPLE 3.7. At the same workshop, there are three round dinner tables, seating twelve people each. The Morris family members (Joy, Dave, and Harmony) still want to sit at the same table, but they have decided to spread out (so no two of them should be side-by-side) to meet more people. How many different seating arrangements are possible at the Morris family's table now?

SOLUTION. Let's begin by arbitrarily placing Joy somewhere at the table, and seating everyone else relative to her. This effectively distinguishes the other eleven seats. Next, we'll consider the nine people who aren't in Joy's family, and place them (standing) in an order clockwise around the table from her. There are $33!/(33-9)!$ ways to do this. Before we actually assign seats to these nine people, we decide where to slot in Dave and Harmony amongst them.



(In the above diagram, the digits 1 through 9 represent the nine other people who are sitting at the Morris family's table, and the J represents Joy's position.) Dave can sit between any pair of non-Morrises who are standing beside each other; that is, in any of the spots marked by small black dots in the diagram above. Thus, there are eight possible choices for where Dave will sit. Now Harmony can go into any of the remaining seven spots marked by black dots. Once Dave and Harmony are in place, everyone shifts to even out the circle (so the remaining black dots disappear), and takes their seats in the order determined.

We have shown that there are $33!/24! \cdot 8 \cdot 7$ possible seating arrangements at the Morris table. That's a really big number, and it's quite acceptable to leave it in this format. However, in case you find another way to work out the problem and want to check your answer, the total number is $783,732,837,888,000$. □

EXERCISES 3.8. Use what you have learned about permutations to work out the following problems. The sum and/or product rule may also be required.

1) Six people, all of whom can play both bass and guitar, are auditioning for a band. There are two spots available: lead guitar, and bass player. In how many ways can the band be completed?

2) Your friend Garth tries out for a play. After the auditions, he texts you that he got one of the parts he wanted, and that (including him) nine people tried out for the five roles. You know that there were two parts that interested him. In how many ways might the cast be completed (who gets which role matters)?

3) You are creating an 8-character password. You are allowed to use any of the 26 lowercase characters, and you must use exactly one digit (from 0 through 9) somewhere in

the password. You are not allowed to use any character more than once. How many different passwords can you create?

4) How many 3-letter "words" (strings of characters, they don't actually have to be words) can you form from the letters of the word STRONG? How many of those words contain an s? (You may not use a letter more than once.)

5) How many permutations of $\{0, 1, 2, 3, 4, 5, 6\}$ have no adjacent even digits? For example, a permutation like 5034216 is not allowed because 4 and 2 are adjacent.

3B. Combinations

Sometimes the order in which individuals are chosen doesn't matter; all that matters is whether or not they were chosen. An example of this is choosing a set of problems for an exam. Although the order in which the questions are arranged may make the exam more or less intimidating, what really matters is which questions are on the exam, and which are not. Another example would be choosing shirts to pack for a trip (assuming all of your shirts are distinguishable from each other). We call a choice like this a "combination," to indicate that it is the collection of things chosen that matters, and not the order.

DEFINITION 3.9. Let n be a positive natural number, and $0 \leq r \leq n$. Assume that we have n distinct objects. An ***r*-combination** of the n objects is a subset consisting of r of the objects.

So a combination involves choosing items from a finite population in which every item is uniquely identified, but the order in which the choices are made is unimportant.

Again, you should not be surprised to learn (since we are studying enumeration) that what we'll be asking is *how many* combinations there are, in a variety of circumstances. One significant difference from permutations is that it's not interesting to ask how many n-combinations there are of n objects; there is only one, as we must choose all of the objects.

Let's begin with an example in which we'll calculate the number of 3-combinations of ten objects (or in this case, people).

EXAMPLE 3.10. Of the ten athletes competing for Olympic medals in women's speed skating (1000 metres), three are to be chosen to form a committee to review the rules for future competitions. How many different committees could be formed?

SOLUTION. We determined in Example 3.2 that there are $10!/7!$ ways in which the medals can be assigned. One easy way to choose the committee would be to make it consist of the three medal-winners. However, notice that if (for example) Wong wins gold, Šajna wins silver, and Andersen wins bronze, we will end up with the same committee as if Šajna wins gold, Andersen wins silver, and Wong wins bronze. In fact, what we've learned about permutations tells us that there are $3!$ different medal outcomes that would each result in the committee being formed of Wong, Šajna, and Andersen.

In fact, there's nothing special about Wong, Šajna, and Andersen – for any choice of three people to be on the committee, there are $3! = 6$ ways in which those individuals could have been awarded the medals. Therefore, when we counted the number of ways in which the medals could be assigned, we counted each possible 3-member committee exactly $3! = 6$ times. So the number of different committees is $10!/(7!3!) = 10 \cdot 9 \cdot 8/6 = 120$. □

We can use the same reasoning to determine a general formula for the number of r-combinations of n objects:

THEOREM 3.11. *The number of r-combinations of n objects is*

$$\frac{n!}{r!(n-r)!}.$$

PROOF. By Theorem 3.3, there are $n!/(n-r)!$ r-permutations of n objects. Suppose that we knew there are k unordered r-subsets of n objects (i.e. r-combinations). For each of these k unordered subsets, there are $r!$ ways in which we could order the elements. This tells us that $k \cdot r! = n!/(n-r)!$. Rearranging the equation, we obtain $k = n!/(r!(n-r)!)$. □

It will also prove extremely useful to have a short form for the number of r-combinations of n objects.

NOTATION 3.12. We use $\binom{n}{r}$ to denote the number of r-combinations of n objects, so

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

DEFINITION 3.13. We read $\binom{n}{r}$ as "***n* choose *r***," so n choose r is $n!/[r!(n-r)!]$.

Notice that when $r = n$, we have

$$\binom{n}{r} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!0!} = \frac{n!}{n!} = 1,$$

coinciding with our earlier observation that there is only one way in which all of the n objects can be chosen. Similarly,

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1;$$

there is exactly one way of choosing none of the n objects.

Let's go over another example that involves combinations.

EXAMPLE 3.14. Jasmine is holding three cards from a regular deck of playing cards. She tells you that they are all hearts, and that she is holding at least one of the two highest cards in the suit (Ace and King). If you wanted to list all of the possible sets of cards she might be holding, how long would your list be?

SOLUTION. We'll consider three cases: that Jasmine is holding the Ace (but not the King); that she is holding the King (but not the Ace), or that she is holding both the Ace and the King.

If Jasmine is holding the Ace but not the King, of the eleven other cards in the suit of hearts she must be holding two. There are $\binom{11}{2}$ possible choices for the cards she is holding in this case.

Similarly, if Jasmine is holding the King but not the Ace, of the eleven other cards in the suit of hearts she must be holding two. Again, there are $\binom{11}{2}$ possible choices for the cards she is holding in this case.

Finally, if Jasmine is holding the Ace and the King, then she is holding one of the other eleven cards in the suit of hearts. There are $\binom{11}{1}$ possible choices for the cards she is holding in this case.

In total, you would have to list

$$\binom{11}{2} + \binom{11}{2} + \binom{11}{1} = \frac{11!}{2!9!} + \frac{11!}{2!9!} + \frac{11!}{1!10!} = \frac{11 \cdot 10}{2} + \frac{11 \cdot 10}{2} + 11 = 55 + 55 + 11 = 121$$

possible sets of cards.

Here is another analysis that also works: Jasmine has at least one of the Ace and the King, so let's divide the problem into two cases: she might be holding the Ace, or she might be holding the King but not the Ace. If she is holding the Ace, then of the twelve other hearts, she is holding two; these can be chosen in $\binom{12}{2} = 66$ ways. If she is holding the King but not the Ace, then as before, her other two cards can be chosen in $\binom{11}{2} = 55$ ways, for a total (again) of 121. □

A common mistake in an example like this, is to divide the problem into the cases that Jasmine is holding the Ace, or that she is holding the King, and to determine that each of these cases includes $\binom{12}{2} = 66$ possible combinations of cards, for a total of 132. The problem with this analysis is that we've counted the combinations that include both the Ace and the King twice: once as a combination that includes the Ace, and once as a combination that includes the King. If you do this, you need to compensate by subtracting at the end the number of combinations that have been counted twice: that is, those that include the Ace and the King. As we worked out in the example, there are $\binom{11}{1} = 11$ of these, making a total of $132 - 11 = 121$ combinations.

EXERCISES 3.15. Use what you have learned about combinations to work out the following problems. Permutations and other counting rules we've covered may also be required.

1) For a magic trick, you ask a friend to draw three cards from a standard deck of 52 cards. How many possible sets of cards might she have chosen?
2) For the same trick, you insist that your friend keep replacing her first draw until she draws a card that isn't a spade. She can choose any cards for her other two cards. How many possible sets of cards might she end up with? (Caution: choosing $5\clubsuit, 6\diamondsuit, 3\spadesuit$ in that order, is *not* different from choosing $6\diamondsuit, 5\clubsuit, 3\spadesuit$ in that order. You do *not* need to take into account that some sets will be more likely to occur than others.)
3) How many 5-digit numbers contain exactly two zeroes? (We insist that the number contain exactly 5 digits.)
4) Sandeep, Hee, Sara, and Mohammad play euchre with a standard deck consisting of 24 cards (A, K, Q, J, 10, and 9 from each of the four suits of a regular deck of playing cards). In how many ways can the deck be dealt so that each player receives 5 cards, with 4 cards left in the middle, one of which is turned face-up? The order of the 3 cards that are left face-down in the middle does not matter, but who receives a particular set of 5 cards (for example, Sara or Sandeep) does matter.
5) An ice cream shop has 10 flavours of ice cream and 7 toppings. Their *megasundae* consists of your choice of any 3 flavours of ice cream and any 4 toppings. (A customer must choose *exactly* three different flavours of ice cream and four different toppings.) How many different megasundaes are there?

3C. The Binomial Theorem

Here is an algebraic example in which "n choose r" arises naturally.

EXAMPLE 3.16. Consider

$$(a+b)^4 = (a+b)(a+b)(a+b)(a+b).$$

If you try to multiply this out, you must systematically choose the a or the b from each of the four factors, and make sure that you make every possible combination of choices sooner or later.

One way of breaking this task down into smaller pieces, is to separate it into five parts, depending on how many of the factors you choose as from (4, 3, 2, 1, or 0). Each time you choose 4 of the as, you will obtain a single contribution to the coefficient of the term a^4; each time you choose 3 of the as, you will obtain a single contribution to the term a^3b; each time you choose 2 of the as, you will obtain a single contribution to the term a^2b^2; each time you choose 1 of the as, you will obtain a single contribution to the term ab^3; and each time you choose 0 of the as, you will obtain a single contribution to the term b^4. In other words, the coefficient of a particular term $a^i b^{4-i}$ will be the number of ways in which you can choose i of the factors from which to take an a, taking a b from the other $4 - i$ factors (where $0 \leq i \leq 4$).

Let's go through each of these cases separately. By Theorem 3.11, there is $\binom{4}{4} = 1$ way to choose four factors from which to take as. (Clearly, you must choose an a from every one of the four factors.) Thus, the coefficient of a^4 will be 1.

If you want to take as from three of the four factors, Theorem 3.11 tells us that there are $\binom{4}{3} = 4$ ways in which to choose the factors from which you take the as. (Specifically, these four ways consist of taking the b from any one of the four factors, and the as from the other three factors). Thus, the coefficient of a^3b will be 4.

If you want to take as from two of the four factors, and bs from the other two, Theorem 3.11 tells us that there are $\binom{4}{2} = 6$ ways in which to choose the factors from which you take the as (then take bs from the other two factors). This is a small enough example that you could easily work out all six ways by hand if you wish. Thus, the coefficient of a^2b^2 will be 6.

If you want to take as from one of the four factors, Theorem 3.11 tells us that there are $\binom{4}{1} = 4$ ways in which to choose the factors from which you take the as. (Specifically, these four ways consist of taking the a from any one of the four factors, and the bs from the other three factors). Thus, the coefficient of ab^3 will be 4.

Finally, by Theorem 3.11, there is $\binom{4}{0} = 1$ way to choose zero factors from which to take as. (Clearly, you must choose a b from every one of the four factors.) Thus, the coefficient of b^4 will be 1.

Putting all of this together, we see that

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

In fact, if we leave the coefficients in the original form in which we worked them out, we see that

$$(a + b)^4 = \binom{4}{4}a^4 + \binom{4}{3}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{1}ab^3 + \binom{4}{0}b^4.$$

This example generalises into a significant theorem of mathematics:

THEOREM 3.17. Binomial Theorem *For any a and b, and any natural number n, we have*

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

One special case of this is that

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

PROOF. As in Example 3.16, we see that the coefficient of $a^r b^{n-r}$ in $(a+b)^n$ will be the number of ways of choosing r of the n factors from which we'll take the a (taking the b from the other $n - r$ factors). By Theorem 3.11, there are $\binom{n}{r}$ ways of making this choice.

For the special case, begin by observing that $(1+x)^n = (x+1)^n$; then take $a = x$ and $b = 1$ in the general formula. Use the fact that $1^{n-r} = 1$ for any integers n and r. □

Thus, the values $\binom{n}{r}$ are the coefficients of the terms in the Binomial Theorem.

DEFINITION 3.18. Expressions of the form $\binom{n}{r}$ are referred to as **binomial coefficients**.

There are some nice, simple consequences of the binomial theorem.

COROLLARY 3.19. *For any natural number n, we have*

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

PROOF. This is an immediate consequence of substituting $a = b = 1$ into the Binomial Theorem. □

COROLLARY 3.20. *For any natural number n, we have*

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

PROOF. From the special case of the Binomial Theorem, we have

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

If we differentiate both sides, we obtain

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

Substituting $x = -1$ gives the result (the left-hand side is zero). □

EXERCISES 3.21. Use the Binomial Theorem to evaluate the following:

1) $\sum_{i=1}^{n} \binom{n}{i} 2^i$.

2) the coefficient of $a^2b^3c^2d^4$ in $(a+b)^5(c+d)^6$.

3) the coefficient of $a^2b^6c^3$ in $(a+b)^5(b+c)^6$.

4) the coefficient of a^3b^2 in $(a+b)^5 + (a+b^2)^4$.

SUMMARY:

- The number of r-permutations of n objects is $n!/(n-r)!$.
- The number of r-combinations of n objects is $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.
- The Binomial Theorem
- Important definitions:
  - permutation, r-permutation
  - n factorial
  - r-combination
  - n choose r
  - binomial coefficients
- Notation:
  - $n!$
  - $\binom{n}{r}$

Chapter 4

Bijections and Combinatorial Proofs

You may recall that in Math 2000 you learned that two sets have the same cardinality if there is a bijection between them. (A bijection is a one-to-one, onto function.) This leads us to another important method for counting a set: we come up with a bijection between the elements of the unknown set, and the elements of a set that we do know how to count. This idea is very closely related to the concept of a combinatorial proof, which we will explore in the second half of this chapter.

Aside: Although we won't explore the concepts of P and NP at all in this course, those of you who have studied these ideas in computer science courses may be interested to learn that most of the techniques used to prove that a particular problem is in P or in NP are related to the techniques discussed in this chapter. Usually a problem X is proven to be in NP (for example) by starting with a problem Y that is already known to be in NP. Then the scientist uses some clever ideas to show that problem Y can be related to problem X in such a way that if problem X could be solved in polynomial time, that solution would produce a solution to problem Y, still in polynomial time. Thus the fact that Y is in NP forces X to be in NP also. The same ideas may sometimes relate the number of solutions of problem X to the number of solutions of problem Y.

4A. Counting via bijections

It can be hard to figure out how to count the number of outcomes for a particular problem. Sometimes it will be possible to find a different problem, and to prove that the two problems have the same number of outcomes (by finding a bijection between their outcomes). If we can work out how to count the outcomes for the second problem, then we've also solved the first problem! This may seem blatantly obvious intuitively, but this technique can provide simple solutions to problems that at first glance seem very difficult.

This technique of counting a set (or the number of outcomes to some problem) indirectly, via a different set or problem, is the bijective technique for counting. We begin with a classic example of this technique.

EXAMPLE 4.1. How many possible subsets are there, from a set of n elements?

SOLUTION. One approach would be to figure out how many 0-element subsets there are, how many 1-element subsets, etc., and add up all of the values we find. This works, but there are so many pieces involved that it is prone to error. Also, the value will not be easy to calculate once n gets reasonably large.

Instead, we imagine creating a table. The columns are indexed by the elements of the set, so there are n columns. We index the rows by the subsets of our set (one per row). In each entry of the table, we place a 1 if the subset that corresponds to this row contains the element that corresponds to this column. Here's an example of such a table when the set is $\{x, y, z\}$:

	x	y	z
$\emptyset$	0	0	0
$\{x\}$	1	0	0
$\{y\}$	0	1	0
$\{z\}$	0	0	1
$\{x, y\}$	1	1	0
$\{x, z\}$	1	0	1
$\{y, z\}$	0	1	1
$\{x, y, z\}$	1	1	1

As you can see, the pattern of 1s and 0s is different in each row of the table, since the elements of each subset are different. Furthermore, any pattern of 1s and 0s that has length 3, appears in some row of this table.

This is not a coincidence. In general, we can define a bijection between the binary strings of length n, and the subsets of a set of n elements, as follows. We already know by the definition of cardinality, that there is a bijection between our set of n elements, and the set $\{1, \ldots, n\}$, so we'll actually define a bijection between the subsets of $\{1, \ldots, n\}$ and the binary strings of length n. Since the composition of two bijections is a bijection, this will indirectly define a bijection between our original set, and the binary strings of length n.

Given a subset of $\{1, \ldots, n\}$, the binary string that corresponds to this subset will be the binary string that has 1s in the ith position if and only if i is in the subset. This tells us how to determine the binary string from the subset. We can also reverse (invert) the process. Given a binary string of length n, the corresponding subset of $\{1, \ldots, n\}$ will be the subset whose elements are the positions of the 1s in the binary string.

Although we haven't directly proven that this map from subsets to binary strings is both one-to-one and onto, an invertible function must be a bijection, so the fact that we were able to find an inverse function does prove that this map is a bijection. (You should check that you agree that the function we've claimed as an inverse really does invert the original function.)

Now, our imaginary table wouldn't be much use if we actually had to write it out. In order to write it out, we would need to know all of the subsets of our set already; and if we knew them all, we could certainly count them! Fortunately, we do not need to write it out. Instead, we use the bijection we have just defined. Rather than count the number of subsets of an n-set, we count the number of binary strings of length n. We can do this using just the multiplication rule! In each position there is either a zero or a one, so there are 2 choices for each of the n positions. Hence, there are 2^n binary strings of length n.

We conclude that 2^n subsets can be formed from a set of cardinality n. □

In some ways, we've actually been using this idea pretty much every time we've come up with more than one way to solve a problem. Implicitly, finding a different way of thinking of the problem is equivalent to finding a bijection between the solutions to these different approaches.

EXAMPLE 4.2. How many ways are there to choose ten people from a group of 30 men and 30 women, if the group must include at least one woman?

SOLUTION. Attacking this problem directly will get ugly. We would have to consider separately the cases of including one woman, two women, etc., all the way up to ten women, in our group, and add all of the resulting terms together. Instead, we note that there is an obvious bijection (the identity map) between groups that *do* include at least one woman, and groups that *do not* include exactly zero women.

The latter is relatively easy to figure out: there are $\binom{60}{10}$ possible groups of ten people that could be chosen from the 60 people. Of these, there are $\binom{30}{10}$ groups that include zero women (since the members of any such group must be chosen entirely from the 30 men). Therefore, the number of groups that do not include exactly zero women, is $\binom{60}{10} - \binom{30}{10}$.

Thanks to our bijection, we conclude that the number of groups that can be chosen, that will include at least one woman, is also $\binom{60}{10} - \binom{30}{10}$. □

EXERCISES 4.3. The following problems should help you in working with the bijective technique for counting.

1) We define a structure that is like a subset, except that any element of the original set may appear 0, 1, or 2 times in the structure. How many of these structures can we form from the set $\{1, \ldots, n\}$?
2) Find a bijection between the coefficient of x^r in $(1+x)^n$, and the number of r-combinations of an n-set.
3) Find a bijection between the number of ways in which three different dolls can be put into ten numbered cribs, and the number of ways in which ten Olympic contenders can win the medals in their event.

4B. Combinatorial proofs

As we said in the previous section, thinking about a problem in two different ways implicitly creates a bijection, telling us that the number of solutions we obtain will be the same either way. When we looked at bijections, we were using this idea to find an easier way to count something that seemed difficult. But if we actually can find a (possibly messy) formula that counts the answer to our problem correctly in some "difficult" way, and we can also find a different formula that counts the answer to the same problem correctly by looking at it in a different way, then we know that the values of the two formulas must be equal, no matter how different they may look.

This is the idea of a "combinatorial proof."

THEOREM 4.4. Combinatorial Proofs *If $f(n)$ and $g(n)$ are functions that count the number of solutions to some problem involving n objects, then $f(n) = g(n)$ for every n.*

DEFINITION 4.5. Suppose that we count the solutions to a problem about n objects in one way and obtain the answer $f(n)$ for some function f; and then we count the solutions to the same problem in a different way and obtain the answer $g(n)$ for some function g. This is a **combinatorial proof** of the identity $f(n) = g(n)$.

The equation $f(n) = g(n)$ is referred to as a **combinatorial identity**.

In the statement of this theorem and definition, we've made f and g functions of a single variable, n, but the same ideas hold if f and g are functions of more than one variable. Our first example demonstrates this.

EXAMPLE 4.6. Prove that for every natural number n and every integer r between 0 and n, we have

$$\binom{n}{r} = \binom{n}{n-r}.$$

COMBINATORIAL PROOF. By the definition of $\binom{n}{r}$, this is the number of ways of choosing r objects from a set of n distinct objects. Any time we choose r of the objects, the other $n-r$ objects are being left out of the set we are choosing. So equivalently, instead of choosing the r objects to include in our set, we could choose the $n-r$ objects to leave out of our set. By the definition of the binomial coefficients, there are $\binom{n}{n-r}$ ways of making this choice.

Therefore, it must be the case that for every natural number n and every integer r between 0 and n, we have

$$\binom{n}{r} = \binom{n}{n-r},$$

as desired. □

Of course, this particular identity is also quite easy to prove directly, using the formula for $\binom{n}{r}$, since

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

Many identities that can be proven using a combinatorial proof can also be proven directly, or using a proof by induction. The nice thing about a combinatorial proof is it usually gives us rather more insight into *why* the two formulas should be equal, than we get from many other proof techniques.

In Example 4.1, we noted that one way to figure out the number of subsets of an n-element set would be to count the number of subsets of each possible size, and add them all up. We then followed a bijective approach to prove that the answer is in fact 2^n. If we actually carry through on the first idea, this leads to another combinatorial identity (one that we already observed via the Binomial Theorem):

EXAMPLE 4.7. Prove that for every natural number n,

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

COMBINATORIAL PROOF. We have seen in Example 4.1 that the number of subsets of a set of n elements is 2^n. We will count the same problem in a different way, to obtain the other side of the equality.

To determine the number of subsets of a set of n elements, we break the problem down into $n+1$ cases, and use the sum rule. The cases into which we will divide the problem are the different possible cardinalities for the subsets: everything from 0 through n. There are $\binom{n}{r}$ ways to choose a subset of r elements from the set of n elements, so the number of subsets that contain r elements is $\binom{n}{r}$. Thus, the total number of subsets of our original set must be $\sum_{r=0}^{n} \binom{n}{r}$.

Since we have counted the same problem in two different ways and obtained different formulas, Theorem 4.4 tells us that the two formulas must be equal; that is,

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

as desired. □

We can also produce an interesting combinatorial identity from a generalisation of the problem studied in Example 4.2.

EXAMPLE 4.8. Suppose we have a collection of n men and n women, and we want to choose r of them for a focus group, but we must include at least one woman. In how many ways can this be done? Use two different methods to count the solutions, and deduce a combinatorial identity.

SOLUTION. Using the same reasoning that we applied in Example 4.2, we see that the number of ways of choosing a group that includes at least one woman is the total number of ways of choosing a group of r people from these $2n$ people, less the number of ways that include only men; that is: $\binom{2n}{r} - \binom{n}{r}$.

Alternatively, we can divide the problem up into r cases depending on how many women are to be included in the group (there must be i women, for some $1 \leq i \leq r$). There are $\binom{n}{i}$ ways to choose i women for the group, and for each of these, there are $\binom{n}{r-i}$ ways to choose $r-i$ men to complete the group. Thus, the total number of ways of choosing a group that includes at least one woman, is

$$\sum_{i=1}^{r} \binom{n}{i}\binom{n}{r-i}.$$

This argument yields the combinatorial identity

$$\sum_{i=1}^{r} \binom{n}{i}\binom{n}{r-i} = \binom{2n}{r} - \binom{n}{r},$$

which we have thereby proven. □

One context in which combinatorial proofs arise very naturally, is when we are counting ordered pairs that have some property. That is, for some subset of $X \times Y$, we may wish to count all of the ordered pairs (x, y), where $x \in X$ and $y \in Y$, such that (x, y) has some property. We can do this by first considering every possible value of $x \in X$, and for each such value, counting the number of $y \in Y$ such that (x, y) satisfies the desired property, or by first considering every possible value of $y \in Y$, and for each such value, counting the number of $x \in X$ such that (x, y) satisfies the desired property.

Although this idea may not seem very practical, it is actually the context in which many of the combinatorial proofs in later chapters will arise. We will be looking at a set X of elements, and a set Y that is actually a collection of subsets of elements of X, and counting pairs (x, y) for which the element x appears in the subset y. By counting these pairs in two ways, we will find a combinatorial identity.

EXAMPLE 4.9. Let B be the set of city blocks in a small city, and let S be the set of street segments in the city (where a street segment means a section of street that lies between two intersections). Assume that each block has at least three sides. Count the number of pairs (s, b) with $s \in S$ and $b \in B$ such that the street segment s is adjacent to the block b in two ways. Use this to deduce a combinatorial inequality.

SOLUTION. Let $|S| = t$. Each street segment is adjacent to two blocks: the blocks that lie on either side of the street. Therefore, for any given street segment s, there are two pairs (s, b) such that s is adjacent to the block b. Multiplying this count by t (the number of street segments) tells us that the total number of pairs $(s, b) \in S \times B$ with s adjacent to b is $2t$.

Let $|B| = c$. Each block is adjacent to at least 3 street segments: the street segments that surround the block. Therefore, for any given block b in the city, there are at least 3 pairs (s, b)

such that b is adjacent to the street segment s. Multiplying this count by c (the number of blocks) tells us that the total number of pairs $(s, b) \in S \times B$ with s adjacent to b is at least $3c$.

We deduce that $2t \geq 3c$. □

EXERCISE 4.10. Let P be the set of people in a group, with $|P| = p$. Let C be a set of clubs formed by the people in this group, with $|C| = c$. Suppose that each club contains exactly g people, and each person is in exactly j clubs. Use two different ways to count the number of pairs $(b, h) \in P \times C$ such that person b is in club h, and deduce a combinatorial identity.

EXERCISES 4.11. Prove the following combinatorial identities, using combinatorial proofs:

1) For any natural numbers r, n, with $1 \leq r \leq n$, $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.
[*Hint:* Consider the number of ways to form a team of r people from a group of n people. Then break the problem into two cases depending on whether or not one specific person is chosen for the team.]

2) For any natural numbers k, r, n, with $0 \leq k \leq r \leq n$, $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$.
[*Hint:* Consider the number of ways to choose r dogs who will enter a competition, from a set of n dogs, and to choose k of those r dogs to become the finalists. Then choose the finalists first, followed by the other dogs who entered the competition.]

3) For any natural number n, $\sum_{r=0}^{n} \binom{n}{r}^2 = \binom{2n}{n}$.

4) For $n \geq 1$ and $k \geq 1$, $\frac{n!}{(n-k)!} = n\frac{(n-1)!}{(n-1-(k-1))!}$.

5) For $n \geq 1$, $3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$.

EXERCISES 4.12. Sometimes the hardest part of a combinatorial proof can be figuring out what problem the given formula provides a solution to. For each of the following formulas, state a counting problem that can be solved by the formula.

1) $n2^{n-1}$.

2) $\sum_{r=0}^{n} r\binom{n}{r}$.

3) $\sum_{k=r}^{n} \binom{n}{k}\binom{k}{r}$.

4) $2^{n-r}\binom{n}{r}$.

SUMMARY:

- Counting via bijections
- Combinatorial identities
- Combinatorial proofs

Chapter 5

Counting with Repetitions

In counting combinations and permutations, we assumed that we were drawing from a set in which all of the elements are distinct. Of course, it is easy to come up with a scenario in which some of the elements are indistinguishable. We need to know how to count the solutions to problems like this, also.

5A. Unlimited repetition

For many practical purposes, even if the number of indistinguishable elements in each class is not actually infinite, we will be drawing a small enough number that we will not run out. The bagel shop we visited in Example 2.8 is not likely to run out of one variety of bagel before filling a particular order. In standard card games, we never deal enough cards to a single player that they might have all of the cards of one suit and still be getting more cards.

This is the sort of scenario we'll be studying in this section. The set-up we'll use is to assume that there are n different "types" of item, and there are enough items of each type that we won't run out. Then we'll choose items, allowing ourselves to repeatedly choose items of the same type as many times as we wish, until the total number of items we've chosen is r. Notice that (unlike in Chapter 3), in this scenario r may exceed n.

We'll consider two scenarios: the order in which we make the choice matters, or the order in which we make the choice doesn't matter.

EXAMPLE 5.1. Chris has promised to bring back bagels for three friends he's studying with (as well as one for himself). The bagel shop sells eight varieties of bagel. In how many ways can he choose the bagels to give to Jan, Tom, Olive, and himself?

SOLUTION. Here, it matters who gets which bagel. We can model this by assuming that the first bagel Chris orders will be for himself, the second for Jan, the third for Tom, and the last for Olive. Thus, the order in which he asks for the bagels matters.

We actually saw back in Chapter 2 how to solve this problem. It's just an application of the product rule! Chris has eight choices for the first bagel; for each of these, he has eight choices for the second bagel; for each of these, he has eight choices for the third bagel; and for each of these, he has eight choices for the fourth bagel. So in total, he has 8^4 ways to choose the bagels. □

OK, so if the order in which we make the choice matters, we just use the multiplication rule. What about if order doesn't matter?

EXAMPLE 5.2. When Chris brought back the bagels, it turned out that he'd done a poor job of figuring out what his friends wanted. They all traded around. Later that night, they sent him to the doughnut store, but this time they told him to just bring back eight doughnuts and they'd figure out who should get which. If the doughnut store has five varieties, how many ways are there for Chris to fill this order?

SOLUTION. Let's call the five varieties chocolate, maple, boston cream, powdered, and jam-filled. One way to describe Chris' order would be to make a list in which we first write one **c** for each chocolate doughnut, then one **m** for each maple doughnut, then one **b** for each boston cream doughnut, then one **p** for each powdered doughnut, and finally one **j** for each jam-filled doughnut. Since Chris is ordering eight doughnuts, there will be eight letters in this list. Notice that there's more information provided by this list than we actually need. We know that all of the first group of letters are **c**s, so instead of writing them all out, we could simply put a dividing marker after all of the **c**s and before the first **m**. Similarly, we can put three more dividing markers in to separate the **m**s from the **b**s, the **b**s from the **p**s, and the **p**s from the **j**s. Now we have a list that might look something like this:

cc||**bbb**|**ppp**|

(Notice in this possible list, Chris chose no maple or jam-filled doughnuts.)

Now, we don't actually need to write down the letters **c**, **m**, **b** and so on, as long as we know how many spaces they take up; we know that any letters that appear before the first dividing marker are **c**s, for example. Thus, the following list gives us the same information as the list above:

__||___|___|

Similarly, if we see the list

|__|__|___|_

we understand that Chris ordered no chocolate doughnuts; two maple doughnuts; two boston cream doughnuts; three powdered doughnuts; and one jam-filled doughnut.

So an equivalent problem is to count the number of ways of arranging eight underlines and four dividing markers in a line. This is something we already understand! We have twelve positions that we need to fill, and the problem is: in how many ways can we fill eight of the twelve positions with underlines (placing dividing markers in the other four positions). We know that this can be done in $\binom{12}{8}$ ways. □

This technique can be used to give us a general formula for counting the number of ways of choosing r objects from n types of objects, where we are allowed to repeatedly choose objects of the same type.

THEOREM 5.3. *The number of ways of choosing r objects from n types of objects (with replacement or repetition allowed) is*

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

PROOF. We use the same idea as in the solution to Example 5.2, above. Since there are n different types of objects, we will need $n-1$ dividing markers to keep them apart. Since we are choosing r objects, we will need r underlines, for a total of $n+r-1$ positions to be filled. We can choose the r positions in which the objects will go in $\binom{n+r-1}{r}$ ways, and then (in each case) put dividing markers into the remaining $n-1$ positions. Thus, there are $\binom{n+r-1}{r}$ ways to choose r objects from n types of objects, if repetition or replacement of choices is allowed. □

Again, we will want to have a short form for this value.

NOTATION 5.4. We use $\left(\!\binom{n}{r}\!\right)$ to denote the number of ways of choosing r objects from n types of objects (with replacement or repetition allowed), so

$$\left(\!\!\binom{n}{r}\!\!\right) = \binom{n+r-1}{r}.$$

The reason we say "replacement or repetition" is because there is another natural model for this type of problem. Suppose that instead of choosing eight bagels from five varieties, Chris is asked to put his hand into a bag that contains five different-coloured pebbles, and draw one out; then replace it, repeatedly (with eight draws in total). If he keeps count of how many times he draws each of the rocks, the number of possible tallies he'll end up with is exactly the same as the number of doughnut orders in Example 5.2.

The following table summarises some of the key things we've learned about counting so far:

Table 5.1. The number of ways to choose r objects from n objects (or types of objects)

	repetition allowed	**repetition not allowed**
order matters	n^r	$\dfrac{n!}{(n-r)!}$
order doesn't matter	$\left(\!\!\binom{n}{r}\!\!\right)$	$\binom{n}{r}$

EXERCISES 5.5. Evaluate the following problems.

1) Each of the ten sections in your community band (trombones, flutes, and so on) includes at least four people. The conductor needs a quartet to play at a school event. How many different sets of instruments might end up playing at the event?
2) The prize bucket at a local fair contains six types of prizes. Kim wins 4 prizes; Jordan wins three prizes, and Finn wins six. Each of the kids plans to give one of the prizes he has won to his teacher, and keep the rest. In how many ways can their prizes (including the gifts to the teacher) be chosen? (It is important which gift comes from which child.)
3) There are three age categories in the local science fair: junior, intermediate, and senior. The judges can choose nine projects in total to advance to the next level of competition, and they must choose at least one project from each age group. In how many ways can the projects that advance be distributed across the age groups?

EXERCISES 5.6. Prove the following combinatorial identities:

1) For $k, n \geq 1$, $\left(\!\binom{n}{k}\!\right) = \left(\!\binom{n-1}{k}\!\right) + \left(\!\binom{n}{k-1}\!\right)$.
2) For $k, n \geq 1$, $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$.
3) For $k, n \geq 1$, $\left(\!\binom{k+1}{n-1}\!\right) = \binom{n+k-1}{k}$.
4) For $1 \leq n \leq k$, $\left(\!\binom{n}{k-n}\!\right) = \binom{k-1}{k-n}$.

EXERCISES 5.7. Solve the following problems.

1) Find the number of 5-lists of the form $(x_1, x_2, x_3, x_4, x_5)$, where each x_i is a nonnegative integer and $x_1 + x_2 + x_3 + x_4 + 3x_5 = 12$.
2) We will buy 3 pies (not necessarily all different) from a store that sells 4 kinds of pie. How many different orders are possible? List all of the possibilities (using A for apple, B for blueberry, C for cherry, and D for the other one).
3) Suppose Lacrosse balls come in 3 colours: red, yellow, and blue. How many different combinations of colours are possible in a 6-pack of Lacrosse balls?
4) After expanding $(a+b+c+d)^7$ and combining like terms, how many terms are there? [Justify your answer without performing the expansion.]

5B. Sorting a set that contains repetition

In the previous section, the new work came from looking at combinations where repetition or replacement is allowed. For our purposes, we assumed that the repetition or replacement was effectively unlimited; that is, the store might only have 30 cinnamon raisin bagels, but since Chris was only ordering four bagels, that limit didn't matter.

In this section, we're going to consider the situation where there are a fixed number of objects in total; some of them are "repeated" (that is, indistinguishable from one another), and we want to determine how many ways they can be arranged (permuted). This can arise in a variety of situations.

EXAMPLE 5.8. When Chris gets back from the doughnut store run, he discovers that Mohammed, Jing, Karl, and Sara have joined the study session. He has bought two chocolate doughnuts, three maple doughnuts, and three boston cream doughnuts. In how many ways can the doughnuts be distributed so that everyone gets one doughnut?

SOLUTION. Initially, this looks a lot like a permutation question: we need to figure out the number of ways to arrange the doughnuts in some order, and give the first doughnut to the first student, the second doughnut to the second student, and so on.

The key new piece in this problem is that, unlike the permutations we've studied thus far, the two chocolate doughnuts are indistinguishable (as are the three maple doughnuts and the three boston cream doughnuts). This means that there is no difference between giving the first chocolate doughnut to Tom and the second to Mohammed, and giving the first chocolate doughnut to Mohammed and the second to Tom.

One way to solve this problem is to look at it as a series of combinations of the people, rather than as a permutation question about the doughnuts. Instead of arranging the doughnuts, we can first choose which two of the eight people will receive the two chocolate doughnuts. Once that is done, from the remaining six people, we choose which three will receive maple doughnuts. Finally, the remaining three people receive boston cream doughnuts. Thus, the solution is $\binom{8}{2}\binom{6}{3}$.

Another approach is more like the approach we used to figure out how many r-combinations there are of n objects. In this approach, we begin by noting that we would be able to arrange the eight doughnuts in 8! orders if all of them were distinct. For any fixed choice of two people who receive the chocolate doughnuts, there are 2! ways in which those two chocolate doughnuts could have been distributed to them, so in the 8! orderings of the doughnuts, each of these choices for who gets the chocolate doughnuts has been counted 2! times rather than once. Similarly, for any fixed choice of three people who receive the maple doughnuts, there are 3! ways in which these three maple doughnuts could have been distributed to them, and each of these choices has been counted 3! times rather than once. The same holds true for the three boston cream doughnuts. Thus, the solution is 8!/(2!3!3!).

Since

$$\binom{8}{2}\binom{6}{3} = \frac{8!}{2!6!} \cdot \frac{6!}{3!3!} = \frac{8!}{2!3!3!},$$

we see that these solutions are in fact identical although they look different. □

This technique can be used to give us a general formula for counting the number of ways of arranging n objects some of which are indistinguishable from each other.

THEOREM 5.9. *Suppose that:*

- *there are n objects;*
- *for each i with $1 \leq i \leq m$, r_i of them are of type i (indistinguishable from each other); and*
- $r_1 + \ldots + r_m = n$.

Then the number of arrangements (permutations) of these n objects is

$$\frac{n!}{r_1!r_2!\ldots r_m!}.$$

PROOF. We use the same idea as in the solution to Example 5.8, above. Either approach will work, but we'll use the first. There will be n positions in the final ordering of the objects. We begin by choosing r_1 of these to hold the objects of type 1. Then we choose r_2 of them to hold the objects of type 2, and so on. Ultimately, we choose the final r_m locations (in $\binom{r_m}{r_m} = 1$ possible way) to hold the objects of type m.

Using the product rule, the total number of arrangements is

$$\begin{aligned} & \binom{n}{r_1}\binom{n-r_1}{r_2}\ldots\binom{n-r_1-\ldots-r_{m-1}}{r_m} \\ = \quad & \frac{n!}{r_1!(n-r_1)!} \cdot \frac{(n-r_1)!}{r_2!(n-r_1-r_2)!} \cdot \ldots \cdot \frac{(n-r_1-\ldots-r_{m-1})!}{r_m!0!} \\ = \quad & \frac{n!}{r_1!r_2!\ldots r_m!}, \end{aligned}$$

since all of the other terms cancel. □

We have notation for this value also.

NOTATION 5.10. We use $\binom{n}{r_1,\ldots,r_m}$ to denote the number of arrangements of $n = r_1 + \ldots + r_m$ objects where for each i with $1 \leq i \leq m$ we have r_i indistinguishable objects of type i. Thus,

$$\binom{n}{r_1,\ldots,r_m} = \frac{n!}{r_1!\ldots r_m!}.$$

This can sometimes apply in unexpected ways.

EXAMPLE 5.11. Cathy, Akos, and Dagmar will be going into a classroom of 30 students. They will each be pulling out four students to work with in a small group setting. In how many ways can the groups be chosen?

SOLUTION. Even though all of the students in the class are distinct, the order in which they get chosen for the group they end up in doesn't matter. One way of making the selection would be to put the names Cathy, Akos, and Dagmar into a hat (four times each) along with 18 blank slips of paper. Each student could choose a slip of paper and would be assigned to the group corresponding to the name they chose. The four slips with Cathy's name on them are identical, as are the four with Akos' name, the four with Dagmar's name, and the 18 blank slips.

Thus, the solution to this problem is

$$\binom{30}{4,4,4,18} = \frac{30!}{4!4!4!18!}.$$

We could also work this out more directly, by allowing each of Cathy, Akos, and Dagmar to choose four students; Cathy's choice can be made in $\binom{30}{4}$ ways; then Akos' in $\binom{26}{4}$ ways; then Dagmar's in $\binom{22}{4}$ ways, and the product of these is $30!/(4!4!4!18!)$. □

EXERCISES 5.12. Evaluate the following problems.

1) Charlie's teacher gives him a set of magnetic words. He has to make a "poem" using all of them. The words are: on, the, one, up, a, tree, the, child, on, jumps, feels, the, child, with. How many different "poems" can Charlie create, if any ordering of the words is considered to be a poem?

2) When filling the soccer team's fundraising order, the chocolate company sent six extra boxes of chocolate-covered almonds, three extra boxes of mints, and two extra boxes of plain chocolate. In how many ways can the extras be fairly distributed to the eleven families who ordered chocolates?

EXERCISES 5.13. Prove the *Multinomial Theorem*: that

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} \prod_{1 \le r \le m} x_r^{k_r}.$$

[*Hint:* Choose arbitrary values for $k_1, k_2, \ldots, k_m$ such that

$$k_1 + k_2 + \cdots + k_m = n,$$

and evaluate the coefficient of $x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}$ that comes from the product on the left-hand side of the equation.]

SUMMARY:

- The number of ways of choosing r objects from n types of objects (with replacement or repetition allowed) is $\left(\!\binom{n}{r}\!\right) = \binom{n+r-1}{r}$.
- The number of ways of arranging n objects where r_i of them are of type i (indistinguishable), is $\binom{n}{r_1,r_2,\ldots,r_m}$.
- Notation:
  - ○ $\left(\!\binom{n}{r}\!\right)$.
  - ○ $\binom{n}{r_1,r_2,\ldots,r_m}$.

Chapter 6

Induction and Recursion

Some problems can most easily be solved (or counted) with the help of a recursively-defined sequence. We'll begin this chapter by introducing these sequences.

You should have seen basic proofs by induction in at least one previous course. Proofs by induction are an important mathematical technique, and are often used in published papers. We'll do a quick review of basic proofs by induction, applying them to recursively-defined sequences. Then we'll touch on some slightly more sophisticated uses of induction. Proofs by induction will be a technique we'll use throughout the remainder of the course, in a variety of contexts.

6A. Recursively-defined sequences

You may be familiar with the term "recursion" as a programming technique. It comes from the same root as the word "recur," and is a technique that involves repeatedly applying a self-referencing definition until we reach some initial terms that are explicitly defined, and then going back through the applications to work out the result we want. If you didn't follow that, it's okay, we'll go through the definition and some specific examples that should give you the idea.

DEFINITION 6.1. A sequence $r_1, r_2, \ldots, r_n, \ldots$ is **recursively defined** if for every n greater than or equal to some bound $b \geq 2$, the value for r_n depends on at least some of the values of $r_1, \ldots, r_{n-1}$. The values for $r_1, \ldots, r_{b-1}$ are given explicitly; these are referred to as the **initial conditions** for the recursively-defined sequence. The equation that defines r_n from $r_1, \ldots, r_{n-1}$ is called the **recursive relation**.

Probably the best-known example of a recursively-defined sequence, is the Fibonacci sequence. It is named for an Italian mathematician who introduced the sequence to western culture as an example in a book he wrote in 1202 to advocate for the use of arabic numerals and the decimal system. The sequence was known to Indian mathematicians as early as the 6th century.

DEFINITION 6.2. The **Fibonacci sequence** is the sequence $f_0, f_1, f_2, \ldots$, defined by $f_0 = 1$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$.

So in the Fibonacci sequence, $f_0 = f_1 = 1$ are the initial conditions, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$ is the recursive relation.

The usual problem associated with recursively-defined sequences, is to find an explicit formula for the nth term that does not require calculating all of the previous terms. Clearly, if we want to be able to determine terms that arise later in the sequence, this is critical. If we try to find the millionth term of a recursively-defined sequence directly, it will require a great deal of computing time and might also require a lot of memory.

Every time you were asked in school to look at a sequence of numbers, find a pattern, and give the next number in the sequence, you were probably working out a recurrence relation and applying it.

EXAMPLE 6.3. Consider the sequence $5, 8, 11, 14$. What number should come next?

SOLUTION. We consider the differences between successive pairs: $8 - 5 = 3$; $11 - 8 = 3$; $14 - 11 = 3$. This appears to be an arithmetic sequence, with the constant difference of 3 between successive terms. So the sequence can be defined by $a_1 = 5$ and $a_n = a_{n-1} + 3$, for every $n \geq 2$. We were asked for a_5, and we know that $a_4 = 14$, so $a_5 = a_4 + 3 = 14 + 3 = 17$.□

Here's a slightly more complicated example:

EXAMPLE 6.4. Consider the sequence $3, 6, 11, 18, 27$. What number should come next?

SOLUTION. Again, consider the differences between successive terms: $6 - 3 = 3$; $11 - 6 = 5$; $18 - 11 = 7$; $27 - 18 = 9$. These differences aren't constant, but do follow a predictable pattern: they are the odd numbers (starting at 3 and increasing). So the sequence can be defined by $a_1 = 3$ and $a_n = a_{n-1} + (2n - 1)$, for every $n \geq 2$. We were asked for a_6, and we know that $a_5 = 27$, so $a_6 = a_5 + 2(6) - 1 = 27 + 11 = 38$. □

This example shows that the recurrence relation can depend on n, as well as on the values of the preceding terms. (Although we didn't state this explicitly in our definition, it is implicit because $n - 1$ is the number of previous terms on which r_n depends; we could calculate n as $a_1^0 + a_2^0 + \ldots + a_{n-1}^0 + 1$.)

Let's look at one more example.

EXAMPLE 6.5. Stavroula's bank pays 1% interest (compounded annually), and charges her a service fee of \$10 per year to maintain the account. The fee is charged at the start of the year, and the interest is calculated on the balance at the end of the year. If she starts with a balance of \$2000, is she making money or losing money? If this account is set up for her by her parents and she's not allowed to touch it, how much money will be in the account after seven years?

SOLUTION. We see that the initial term is $r_0 = 2000$. We're going to use r_0 as the first term, because then the value of her account after 1 year will be r_1; after two years will be r_2; and after seven years will be r_7. This just makes it a little easier to keep track of what we're aiming to figure out.

If we unpack the financial language, it is telling us that every year, the bank takes \$10 from Stavroula's account at the start of the year. Then at the end of the year, the bank adds 1% of whatever is in Stavroula's account, to her account. This can be represented by the following recurrence relation: $r_n = r_{n-1} - 10 + .01(r_{n-1} - 10)$ for every $n \geq 1$, which simplifies to $r_n = 1.01(r_{n-1} - 10)$. Logically, she will be making money if the 1% that she earns in interest, exceeds the service fee of \$10, so if she makes money in the first year, she will continue to make money; while if she loses money in the first year, she will continue to lose money after that. So to answer the first question, we'll work out $r_1 = 1.01(r_0 - 10) = 1.01(1990) = 2009.9$. Stavroula is making money.

To answer the second question, unless we've managed to figure out an explicit formula for r_n (which we don't yet know how to do), we need to calculate r_2, r_3, r_4, r_5, r_6, and r_7. It would be reasonable to assume that the bank rounds its calculations to the nearest penny every year, and carries forward with the rounded value, but because this will create an error that will be compounded in comparison with solving our recurrence relation explicitly (which we'll learn later how to do), we'll keep track of the exact values instead. We have

$$\begin{aligned}
r_2 &= 1.01(2009.9-10) = 2019.899;\\
r_3 &= 1.01(2009.899) = 2029.99799;\\
r_4 &= 1.01(2019.99799) = 2040.1979699;\\
r_5 &= 1.01(2030.1979699) = 2050.499949599;\\
r_6 &= 1.01(2040.499949599) = 2060.90494909499;\ \text{and}\\
r_7 &= 1.01(2050.90494909499) = 2071.4139985859399.
\end{aligned}$$

So at the end of seven years, Stavroula has \$2071.41. □

EXERCISES 6.6. Solve the following problems about recurrence relations.

1) Consider the sequence $4, 9, 19, 39$. Give a recurrence relation that describes this sequence, and find the next term in the sequence.
2) Use the recurrence relation for the Fibonacci sequence to find f_6.
3) If the annual fee on Stavroula's bank account from Example 6.5 is \$20 instead of \$10, is she making money or losing money?

6B. Basic induction

Suppose we want to show that $n!$ is at least $2^n - 2$, for every $n \geq 1$ (where n must be an integer). We could start verifying this fact for each of the possible values for n:

$$\begin{aligned}
1! &= 1 \geq 2^1 - 2 = 0;\\
2! &= 2 \geq 2^2 - 2 = 2;\\
3! &= 6 \geq 2^3 - 2 = 6;\\
4! &= 24 \geq 2^4 - 2 = 14.
\end{aligned}$$

We could continue verifying the values one at a time, but the process would go on forever, so we'd never be able to complete the proof.

Instead, think about the following method. We know that the inequality holds for $n = 1$. Let's suppose that the inequality holds for some value $n = k$, i.e. that

$$k! \geq 2^k - 2.$$

Now let's use the fact that we can easily calculate $(k+1)!$ from $k!$ together with our supposition, to deduce that the inequality holds when $n = k + 1$, i.e. that

$$(k+1)! \geq 2^{k+1} - 2.$$

This is enough to prove the inequality for every integer $n \geq 1$, because applying our supposition and deduction enough times will prove the inequality for any value at all that interests us! For example, if we wanted to be sure that the inequality holds for $n = 100$, we could take the fact that we know it holds for 1, to deduce that it holds for 2, then the fact that it holds for 2 allows us to deduce that it holds for 3. By repeating this 97 more times, eventually we see that since it holds for 99, we can deduce that it holds for 100.

THEOREM 6.7. Principle of Mathematical Induction *Let $P(n)$ be an assertion about the integer n. If we know that*

1) *the assertion $P(n_0)$ is true for some particular integer n_0; and*
2) *for any integer $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ must also be true,*

then $P(n)$ is true for every integer $n \geq n_0$.

DEFINITION 6.8. In a proof by induction, determining that $P(n_0)$ is true for some particular integer n_0 is called the **base case**. Proving the conditional statement that $P(k) \Rightarrow P(k+1)$ for every $k \geq n_0$ is called the **inductive step**. The assumption we make in the inductive step, that $P(k)$ is true for some arbitrary $k \geq n_0$, is called the **inductive hypothesis**, and can be referred to by (IH) when it is being used in the proof.

Now that we've gone through the formalities, let's write a proper proof by induction for the inequality we used to introduce this idea.

EXAMPLE 6.9. Prove by induction that $n! \geq 2^n - 2$, for every integer $n \geq 2$. (This inequality is actually true for every $n \geq 0$, but the proof is considerably simpler if we restrict our attention to $n \geq 2$.)

SOLUTION. Proof. Base case: $n = 2$. We have $n! = 2! = 2$, and

$$2^n - 2 = 2^2 - 2 = 4 - 2 = 2.$$

Certainly $2 \geq 2$, so the inequality holds for $n = 2$. This completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 2$ be arbitrary, and suppose that the inequality holds for $n = k$; that is, assume that $k! \geq 2^k - 2$.

Now we want to deduce that

$$(k+1)! \geq 2^{k+1} - 2.$$

Let's start from the left-hand side of this inequality. By the definition of factorial, we know that

$$(k+1)! = (k+1)k!.$$

Now that we have $k!$ in the expression, we're in a position to apply the inductive hypothesis; that is,

$$(k+1)! = (k+1)k! \geq (k+1)(2^k - 2).$$

Since $k \geq 2$, we have $k + 1 \geq 3$, so

$$(k+1)(2^k - 2) \geq 3(2^k - 2) = 2(2^k) + 2^k - 6 = 2^{k+1} + 2^k - 6.$$

Again, since $k \geq 2$, we have $2^k \geq 4$, so $2^k - 6 \geq -2$. Hence

$$(k+1)! \geq 2^{k+1} + 2^k - 6 \geq 2^{k+1} - 2,$$

which is what we wanted to deduce. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $n! \geq 2^n - 2$ for every integer $n \geq 2$. □

Proofs by induction work very naturally with recursively-defined sequences, since the recurrence relation gives us information about the $(k+1)$st term of the sequence, based on previous terms.

EXAMPLE 6.10. Consider the sum of the first n integers. We can think about this as a recursively-defined sequence, by defining $s_1 = 1$, and $s_n = s_{n-1} + n$, for every $n \geq 2$. Thus, $s_2 = 1 + 2$;

$$s_3 = s_2 + 3 = 1 + 2 + 3,$$

and so on. Prove by induction that $s_n = n(n+1)/2$, for every $n \geq 1$.

SOLUTION. Proof. Base case: $n = 1$. We have $s_n = s_1 = 1$, and

$$n(n+1)/2 = 1(2)/2 = 1,$$

so the equality holds for $n = 1$. This completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 1$ be arbitrary, and suppose that the equality holds for $n = k$; that is, assume that $s_k = k(k+1)/2$.

Now we want to deduce that

$$s_{k+1} = (k+1)(k+2)/2.$$

Using the recursive relation, we have $s_{k+1} = s_k + (k+1)$ since $k+1 \geq 2$, and using the inductive hypothesis, we have $s_k = k(k+1)/2$, so putting these together, we see that

$$s_{k+1} = k(k+1)/2 + (k+1).$$

Taking out a common factor of $k+1$ gives

$$s_{k+1} = (k+1)(k/2+1) = (k+1)(k+2)/2,$$

which is what we wanted to deduce. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $s_n = n(n+1)/2$ for every $n \geq 1$. □

Caution: the steps of a proof by induction are precisely defined, and if you leave any of them out, or forget the conditions required, things can go badly wrong. The base case may seem obvious, but can't be left out; also, the hypothesis that $k \geq n_0$ may be critical to the proof, as we saw in Example 6.9.

Let's look at an example where, by forgetting to include the base case, we can give a "proof by induction" of something that is clearly false.

EXAMPLE 6.11. Here is a "proof by induction" (without a base case) that every integer n is at least 1000.

PROOF. Inductive step: We begin with the inductive hypothesis. Let k be arbitrary, and suppose that $k \geq 1000$.

Now we want to deduce that $k+1 \geq 1000$. But clearly,

$$k+1 \geq k \geq 1000$$

(by our inductive hypothesis), which is what we wanted to deduce. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $n \geq 1000$ for every integer n. □

Now it's your turn to try a few, but don't leave out any of the steps!

EXERCISES 6.12. Use the Principle of Mathematical Induction to prove the following:

1) For the recursively-defined sequence given by $b_1 = 5$ and $b_n = b_{n-1} + 4$ for all $n \geq 2$, prove that for every integer $n \geq 1$, $b_n = 5 + 4(n-1)$.
2) For the recursively-defined sequence given by $c_1 = 3$ and $c_n = c_{n-1} + 3 \cdot 2^{n-1}$ for all $n \geq 2$, prove that for every integer $n \geq 1$, $c_n = 3(2^n - 1)$.
3) Prove that for every integer $n \geq 0$, $n! \geq n$.
4) Prove that for every integer $n \geq 0$, $4^n - 1$ is divisible by 3.
5) Starting with $n = 2$ and increasing n from there, calculate the first few values for the product

$$t_n = \prod_{j=2}^{n} (1 - \frac{1}{j}).$$

Conjecture a closed formula for t_n based on the values you have calculated, and use induction to prove that your formula is correct.

6) Prove that for every integer $n \geq 1$,

$$\sum_{j=1}^{n} j! \leq \frac{1}{2}(n+1)!$$

7) Define $c_0 = 1$ and for $n \geq 1$, define $c_n = nc_{n-1} + 1$. Prove by induction: for $n \geq 0$,

$$c_n = \sum_{j=0}^{n} \frac{n!}{(n-j)!}.$$

6C. More advanced induction

Now that we've reviewed the basic form of induction, it's important to consider some more advanced forms that are often used.

The first form we'll look at is strong induction. When we have a recursively-defined sequence that depends on the previous terms, sometimes we need to know not just about the single term that comes immediately before the nth term, but about other previous terms. Only by putting all of this information together will we be able to deduce the result we need about the nth term.

EXAMPLE 6.13. Let's define a recursively-defined sequence by $a_1 = 2$ and for every integer $n \geq 2$, we have

$$a_n = \sum_{i=1}^{n-1} a_i.$$

Thus, $a_2 = a_1 = 2$;

$$\begin{aligned} a_3 &= a_1 + a_2 = 2 + 2 = 4; \\ a_4 &= a_1 + a_2 + a_3 = 2 + 2 + 4 = 8, \end{aligned}$$

and so on. Prove by induction that for every $n \geq 2$, we have $a_n = 2^{n-1}$.

SOLUTION ATTEMPT. We begin with the base case: when $n = 2$, we have $a_2 = 2 = 2^{2-1}$, so the equality is true for the base case. Now for the inductive hypothesis, we let $k \geq 2$ be arbitrary, and suppose that the equality is true for $n = k$, so $a_k = 2^{k-1}$. Now when $n = k + 1$, we have

$$a_n = a_{k+1} = \sum_{i=1}^{k} a_i,$$

by the recursive relation for this sequence. We know what a_1 is, by our initial condition; we know that $a_k = 2^{k-1}$, but what about the values in between? The Principle of Mathematical Induction as we've learned it so far, doesn't allow us to assume anything about (for example) a_{k-1}.

Actually, though, the way the concept of induction works, by the time we're trying to prove something about a_n, we've actually already deduced it for *every* value between n_0 and $n - 1$(inclusive). So there is nothing wrong with assuming that $P(i)$ is true for every value between n_0 and k, rather than just for k, in order to deduce that $P(k + 1)$ is true. More concretely, this is saying the following. Suppose that by knowing $P(0)$ we can deduce $P(1)$, and then by knowing $P(0)$ *and* $P(1)$ we can deduce $P(2)$, and so on, so that eventually by knowing that everything from $P(0)$ through $P(k)$ is true, we can deduce that $P(k+1)$ is true.

Then $P(n)$ is true for every integer $n \geq 0$. Of course, we don't have to start with 0; we can start with any integer n_0. This is the strong form of mathematical induction:

THEOREM 6.14. Strong Induction *Suppose we have a statement $P(n)$ about the integer n. If we know that*

1) the statement $P(n_0)$ is true for some particular integer n_0; and

2) for any integer $k \geq n_0$, if every $P(i)$ is true for $n_0 \leq i \leq k$, then $P(k+1)$ must also be true,

then $P(n)$ is true for every integer $n \geq n_0$.

Using this, we can complete the example we started above. We have $a_1 = 2$ (by the initial condition), and the strong induction hypothesis allows us to assume that $a_i = 2^{i-1}$ for every integer i with $2 \leq i \leq k$. So using the recursive relation

$$a_{k+1} = \sum_{i=1}^{k} a_i,$$

we see that

$$a_{k+1} = 2 + \sum_{i=2}^{k} 2^{i-1}.$$

You probably learned in high school how to add up geometric sequences like this; in particular, that

$$\sum_{j=0}^{k} 2^j = 2^{k+1} - 1,$$

and we can re-write what we have as

$$a_{k+1} = 1 + \left(1 + \sum_{j=1}^{k-1} 2^j\right) = 1 + \sum_{j=0}^{k-1} 2^j = 1 + \left(2^{(k-1)+1} - 1\right) = 2^k.$$

This is precisely what we needed to deduce, so this completes the proof.

Let's go over one more example that involves strong induction. In this example, we'll need strong induction for a slightly different reason: we'll need the statement to be true for some values between n_0 and k, but we're not necessarily sure which ones.

EXAMPLE 6.15. Shawna is building a tower with lego. Prove that if she has n pieces of lego (where $n \geq 1$), and a "move" consists of sticking two smaller towers together into one (where a tower may consist of one or more pieces of lego), then it will take her $n - 1$ moves to complete the tower.

SOLUTION. Proof. Base case: $n = 1$. Shawna's "tower" is already complete after $n - 1 = 0$ moves. This completes the proof of the base case.

Induction step: we begin with the induction hypothesis, that when $1 \leq i \leq k$, it takes Shawna $i - 1$ moves to build a tower that contains i pieces of lego.

Now we want to deduce that when Shawna has $k + 1$ pieces of lego, it takes her k moves to stick them together into a single tower. Notice that when she makes her final move, it must consist of sticking together two smaller towers, one of which contains j pieces of lego, and the other of which contains the remaining $k+1-j$ pieces. Both j and $k+1-j$ must lie between 1 and k (if either of the smaller towers had $k+1$ pieces then the tower would already be complete), so the induction hypothesis applies to each of them. Thus, it has taken Shawna $j - 1$ moves to build the tower that contains j pieces, and $k-j$ moves to build the tower that contains $k-j+1$ pieces. Together with her final move, then, it must take Shawna

$$(j-1)+(k-j)+1$$

moves in total to complete her tower of $k+1$ pieces. Now,

$$(j-1)+(k-j)+1=k,$$

so it takes Shawna k moves to complete the tower, which is what we wanted to deduce. This completes the proof of the inductive step.

By Strong Induction, it will take Shawna $n-1$ moves to complete a tower that contains n blocks of lego, for every $n \geq 1$. □

This is pretty amazing. If we tried to go through the full argument for how many moves it takes her to build a tower with four blocks, it would go something like this. First, to build a tower with one block clearly takes 0 moves; to build a tower with two blocks clearly takes 1 move (stick the two blocks together). To build a tower with three blocks, we must use 1 move to stick together a tower of two blocks (which took 1 move to create) with a tower of one block (which took 0 moves to create), meaning that we use 2 moves altogether. Now, a tower of four blocks can be built in two ways: by using 1 move to stick together two towers of two blocks, each of which took 1 move to make, for a total of 3 moves; or by using 1 move to stick together a tower of one block (which took 0 moves to make) with a tower of three blocks (which took 2 moves to make), for a total of 3 moves. So under either method, building a tower of four blocks takes 3 moves. You can see that the argument will get more and more complicated as n increases, but it will always continue to work.

We won't need strong induction as such very much until later in the course, but the idea is useful background for the next kind of induction we'll look at, which is very important when dealing with recurrence relations: induction with multiple base cases.

Induction with multiple base cases is very important for dealing with recursively-defined sequences such as the Fibonacci sequence, where each term depends on more than one of the preceding terms.

Suppose you were asked to prove that the nth term of the Fibonacci sequence, f_n, is at least 2^{n-2}. If we try to follow our basic inductive strategy, we'd begin by observing that this is true for f_0:

$$f_0 = 1 \geq 2^{-2} = 1/4.$$

Then we'd make the inductive hypothesis that our inequality is true for some arbitrary $k \geq 0$, so $f_k \geq 2^{k-2}$. Now to deduce the inequality for $n = k+1$, the natural approach is to use the recursive relation, which tells us that

$$f_{k+1} = f_k + f_{k-1}.$$

We can use our inductive hypothesis to make a substitution for f_k, but what about f_{k-1}? You might (reasonably) argue at this point that we should use strong induction, which will allow us to assume that the result is true for both f_k and f_{k-1}, but actually, this doesn't work! Why not? Well, the trouble is that everything we know about the Fibonacci sequence starts with f_0, but if $k = 1$ (which is the first time we try to use induction) then $f_{k-1} = f_{-1}$, which we haven't even defined! It is very important to ensure that in the inductive step, we never make our assumption go back *too far*, i.e. to a value below n_0.

So, how can we deal with this problem? The solution is to add another base case, for $n = 1$. When $n = 1$, we have

$$f_1 = 1 \geq 2^{1-2} = 1/2.$$

Now if we try induction, at the first step we will be using the fact that the statement is true for f_0 and f_1 to prove it for f_2; then the fact that it's true for f_1 and f_2 will allow us to deduce it for f_3, and so on. The final argument will look like the following.

EXAMPLE 6.16. Prove by induction that the nth term of the Fibonacci sequence, f_n, is at least $(3/2)^{n-1}$, for every $n \geq 0$.

SOLUTION. Since the recursive relation for the Fibonacci sequence requires the two immediately preceding terms, we will require two base cases.

Proof. Base cases: When $n = 0$, we have

$$f_0 = 1 \geq (3/2)^{-1} = 2/3,$$

so the inequality holds for $n = 0$. When $n = 1$, we have

$$f_1 = 1 \geq (3/2)^{1-1} = 1,$$

so the inequality holds for $n = 1$. This completes the proof of the base cases.

Inductive step: We begin with the (strong) inductive hypothesis. Let k be an arbitrary integer at least as big as our biggest base case, so $k \geq 1$. Assume that for every integer i with $0 \leq i \leq k$, we have $f_i \geq (3/2)^{i-1}$.

Now we want to deduce that

$$f_{k+1} \geq (3/2)^{(k+1)-1} = (3/2)^k.$$

Using the recursive relation, we know that $f_{k+1} = f_k + f_{k-1}$. Since $k \geq 1$, we have $k - 1 \geq 0$, so both k and $k - 1$ satisfy the bounds on i (that $0 \leq i \leq k$), so that we can apply our inductive hypothesis to both f_k and f_{k-1}. We therefore have

$$f_{k+1} \geq \left(\frac{3}{2}\right)^{k-1} + \left(\frac{3}{2}\right)^{k-2} = \left(\frac{3}{2} + 1\right)\left(\frac{3}{2}\right)^{k-2} = \frac{5}{2}\left(\frac{3}{2}\right)^{k-2} = \frac{5}{3} \cdot \frac{3}{2}\left(\frac{3}{2}\right)^{k-2} > \left(\frac{3}{2}\right)^{k},$$

since $5/3 > 3/2$. This is what we wanted to deduce. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $f_n \geq (3/2)^{n-1}$ for every $n \geq 0$. □

EXERCISES 6.17.

1) Prove by induction that for every $n \geq 0$, the nth term of the Fibonacci sequence is no greater than 2^n.

2) The machine at the coffee shop isn't working properly, and can only put increments of \$4 or \$5 on your gift card. Prove by induction that you can get any amount of dollars that is at least \$12.

   [*Hint:* You should have four base cases.]

3) Define a recurrence relation by $a_0 = a_1 = a_2 = 1$, and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n \geq 3$. Prove by induction that $a_n \leq 2^n$ for all $n \geq 0$.

SUMMARY:

- Important definitions:
  - recursively-defined sequence
  - initial conditions
  - recursive relation
  - Fibonacci sequence
  - proof by induction
  - base case
  - inductive step
  - inductive hypothesis
  - strong induction
  - induction with multiple base cases
- Notation:
  - (IH)

Chapter 7

Generating Functions

Recall that the basic goal with a recursively-defined sequence, is to find an explicit formula for the nth term of the sequence. Generating functions will allow us to do this.

7A. What is a generating function?

A generating function is a formal structure that is closely related to a numerical sequence, but allows us to manipulate the sequence as a single entity, with the goal of understanding it better. Here's the formal definition.

DEFINITION 7.1. For a sequence $a_0, a_1, \ldots, a_n, \ldots$ the corresponding **generating function** $f(x)$ is the series

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots = \sum_{i=0}^{\infty} a_i x^i.$$

So a_n, the nth term of the sequence, is the coefficient of x^n in $f(x)$.

EXAMPLE 7.2. Here are a number of basic examples.

1) $1, 1, 1, 1, 1, 1, 0, 0, 0, \ldots$ has generating function

$$1 + x + x^2 + x^3 + x^4 + x^5.$$

2) $1, 4, 6, 4, 1, 0, 0, 0, \ldots$ has generating function

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

3) $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}, 0, 0, 0, \ldots$ has generating function

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

4) $1, 1, 1, 1, \ldots$ has generating function

$$f(x) = 1 + x + x^2 + x^3 + \ldots = \sum_{i=0}^{\infty} x^i.$$

These generating functions can be manipulated. For example, if $f(x)$ is as in Example 7.2(4), suppose we take the product $(1-x)f(x)$. We have

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

Dividing through by $1-x$, we see that $f(x) = 1/(1-x)$.

This may seem artificial and rather nonsensical since the generating function was defined as a formal object whose coefficients are a sequence that interests us. In fact, although we won't delve into the formalities in this course, algebraic manipulation of generating functions can be formally defined, and gives us exactly these results.

A reasonable question at this point might be, what use is this? Even if we agree that $f(x) = 1/(1-x)$, what we really want is the coefficient of x^n (in order to retrieve a_n, the nth term of our sequence). If we have an expression like $1/(1-x)$, how can we work out the coefficient of x^n?

EXERCISES 7.3. For each of the following sequences, give the corresponding generating function.

1) $1, 3, 5, 0, 0, 0, \dots$.
2) $1, 2, 2^2, 2^3, 2^4, \dots$.
3) $1, 5, 10, 15, 10, 5, 1, 0, 0, 0, \dots$.
4) $1, 5, 10, 10, 5, 1, 0, 0, 0, \dots$.

7B. The Generalised Binomial Theorem

We are going to present a generalised version of the special case of Theorem 3.17, the Binomial Theorem, in which the exponent is allowed to be negative. Recall that the Binomial Theorem states that

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

If we have $f(x)$ as in Example 7.2(4), we've seen that

$$f(x) = 1/(1-x) = (1-x)^{-1}.$$

So if we were allowed negative exponents in the Binomial Theorem, then a change of variable $y = -x$ would allow us to calculate the coefficient of x^n in $f(x)$.

Of course, if n is negative in the Binomial Theorem, we can't figure out anything unless we have a definition for what $\binom{n}{r}$ means under these circumstances.

DEFINITION 7.4. The **generalised binomial coefficient**,

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

where $r \geq 0$ but n can be any real number.

Notice that this coincides with the usual definition for the binomial coefficient when n is a positive integer, since

$$n!/(n-r)! = n(n-1)\dots(n-r+1)$$

in this case.

EXAMPLE 7.5.

$$\binom{-2}{5} = \frac{(-2)(-3)(-4)(-5)(-6)}{5!} = -6.$$

If n is a positive integer, then we can come up with a nice formula for $\binom{-n}{r}$.

PROPOSITION 7.6. *If n is a positive integer, then*

$$\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}.$$

PROOF. We have

$$\binom{-n}{r} = \frac{-n(-n-1)\ldots(-n-r+1)}{r!}.$$

Taking a factor of (-1) out of each term on the right-hand side gives

$$(-1)^r n(n+1)\ldots(n+r-1)/(r!).$$

Now,

$$(n+r-1)(n+r-2)\ldots n = (n+r-1)!/(n-1)!,$$

so

$$(-1)^r \frac{n(n+1)\ldots(n+r-1)}{r!} = (-1)^r \frac{(n+r-1)!}{r!(n-1)!} = (-1)^r \binom{n+r-1}{r},$$

as claimed. □

With this definition, the binomial theorem generalises just as we would wish. We won't prove this.

THEOREM 7.7. Generalised Binomial Theorem *For any $n \in \mathbb{R}$,*

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

EXAMPLE 7.8. Let's check that this gives us the correct values for the coefficients of $f(x)$ in Example 7.2(4), which we already know.

SOLUTION. We have

$$f(x) = (1-x)^{-1} = (1+y)^{-1},$$

where $y = -x$. The Generalised Binomial Theorem tells us that the coefficient of y^r will be

$$\binom{-1}{r} = (-1)^r \binom{1+r-1}{r} = (-1)^r,$$

since $\binom{r}{r} = 1$. But we want the coefficient of x^r, not of y^r, and

$$y^r = (-x)^r = (-1)^r x^r,$$

so we have

$$(-1)^r y^r = (-1)^{2r} x^r = 1^r x^r = x^r.$$

Thus, the coefficient of x^r in $f(x)$ is 1. This is, indeed, precisely the sequence we started with in Example 7.2(4). □

EXAMPLE 7.9. Let's work out $(1+x)^{-3}$.

SOLUTION. We need to know what $\binom{-3}{r}$ gives, for various values of r. By Proposition 7.6, we have

$$\binom{-3}{r} = (-1)^r \binom{3+r-1}{r} = (-1)^r \binom{r+2}{r} = (-1)^r \frac{(r+2)(r+1)}{2}.$$

When $r = 0$, this is $(-1)^0 2 \cdot 1/2 = 1$. When $r = 1$, this is $(-1)^1 3 \cdot 2/2 = -3$. When $r = 2$, this is $(-1)^2 4 \cdot 3/2 = 6$. In general, we see that

$$(1+x)^{-3} = 0 - 3x + 6x^2 - + \ldots + (-1)^n \frac{(n+2)(n+1)}{2} x^n + \ldots \qquad \square$$

EXERCISES 7.10. Calculate the following.

1) $\binom{-5}{7}$
2) The coefficient of x^4 in $(1-x)^{-2}$.
3) The coefficient of x^n in $(1+x)^{-4}$.
4) The coefficient of x^{k-1} in
$$\frac{1+x}{(1-2x)^5}.$$
Hint: Notice that $\frac{1+x}{(1-2x)^5} = (1-2x)^{-5} + x(1-2x)^{-5}$. Work out the coefficient of x^n in $(1-2x)^{-5}$ and in $x(1-2x)^{-5}$, substitute $n = k-1$, and add the two coefficients.
5) The coefficient of x^k in $1/(1-x^j)^n$, where j and n are fixed positive integers.
Hint: Think about what conditions will make this coefficient zero.

7C. Using generating functions to count things

As you might expect of something that has come up in our study of enumeration, generating functions can be useful in solving problems about counting. We've already seen from the Binomial Theorem, that the coefficient of x^r in $(1+x)^n$, is $\binom{n}{r}$, so the generating function for the binomial coefficients is $(1+x)^n$. In fact, the argument we used to prove the Binomial Theorem explained why this works: if we want the coefficient of x^r in $(1+x)^n$, it must be the number of ways of choosing the x from r of the n factors, while choosing the 1 from the other factors. We can use similar reasoning to solve other counting questions.

EXAMPLE 7.11. The grocery store sells paper plates in packages of 1, 5, 20, or 75. In how many different ways can Jiping buy a total of 95 paper plates?

SOLUTION. We model this with generating functions. The exponent of x will represent the number of paper plates, and the coefficient of x^n will represent the number of ways in which he can buy n paper plates.

We begin by considering the single paper plates that he buys. He could buy 0, or 1, or any other number of these, so we represent this by the generating function

$$1 + x + x^2 + x^3 + x^4 + \ldots = \sum_{i=0}^{\infty} x^i = 1/(1-x).$$

There is exactly one way of choosing any particular number of single paper plates (we are assuming the plates are indistinguishable).

Now, he could also buy any number of packages of 5 paper plates, but the difference is that each package he buys contributes 5 to the exponent, since it represents 5 plates. We represent this by the generating function

$$1 + x^5 + x^{10} + x^{15} + \ldots = \sum_{i=0}^{\infty} x^{5i} = 1/(1-x^5),$$

where i represents the number of packages he buys.

Similarly, he could buy any number of packages of 20 paper plates, and each package he buys contributes 20 to the exponent, since it represents 20 plates. We represent this by the generating function

$$1 + x^{20} + x^{40} + x^{60} + \ldots = \sum_{i=0}^{\infty} x^{20i} = 1/(1-x^{20}),$$

where i represents the number of packages he buys.

Finally, he could buy any number of packages of 75 paper plates, and each package he buys contributes 75 to the exponent, since it represents 75 plates. We represent this by the generating function

$$1 + x^{75} + x^{150} + x^{225} + \ldots = \sum_{i=0}^{\infty} x^{75i} = 1/(1-x^{75}),$$

where i represents the number of packages he buys.

Obviously, for this particular question, Jiping can't actually buy 2 or more of the packages of 75 paper plates, since that would be too many. There are also limits on the number of packages of other sizes that he should buy, since he doesn't want to end up with more than 95 plates. So for this problem, we can assume that the generating function for the full problem actually looks like this:

$$(1 + x + x^2 + \ldots + x^{95})(1 + x^5 + x^{10} + \ldots + x^{95})(1 + x^{20} + x^{40} + x^{60} + x^{80})(1 + x^{75})$$

and we are looking for the coefficient of x^{95}.

We could multiply this all out to get our answer. We could be a bit more clever, recognising that we only really care about the coefficient of x^{95}, and break the problem down into cases depending on how many of the bigger packages he buys. It should be noted that the generating function hasn't really saved us any work. This approach involves saying, "Well, if he takes the x^{75} from the final factor, then there are only six ways to contribute to the coefficient of x^{95}: he could choose an x^{20} from the previous factor and 1s from both of the other factors; or he could choose 1 from the third factor and any of 1, x^5, x^{10}, x^{15}, or x^{20} from the second factor, in each case choosing whichever term from the first factor brings the exponent up to 95." This is exactly equivalent to saying, "Well, if he buys a package of 75 plates, then there are only six ways to buy 95 plates in total: he could buy a package of 20 plates and be done; or he could buy 0, 1, 2, 3, or 4 packages of 5 plates, in each case buying as many single plates as are needed to bring the total up to 95."

So what's the advantage of the generating function approach? It comes in a couple of ways. First, it solves multiple problems at once: if we actually multiply out the generating function above, we will be able to read off not only how many ways there are of buying 95 plates, but also how many ways there are of buying every number of plates up to 95. (If we hadn't cut the factors off as we did, we could also work out the answers for any number of plates higher than 95.) So by doing a bunch of multiplication once (and it's easy to feed into a computer algebra system if you don't want to do it by hand), we can simultaneously find out the answer to a lot of closely-related questions.

The other advantage is that the generating function approach can help us solve problems that we don't see how to solve without it, such as finding an explicit formula for the nth term of a recursively-defined sequence. □

Here's an example that involves working out the coefficient of a term in a generating function in two different ways.

EXAMPLE 7.12. Consider the generating function $(1/(1-x))^4 = (1+x+x^2+x^3+\ldots)^4$. As usual, we want to determine the coefficient of x^r in this product.

SOLUTION. We must choose a power of x from each of the four factors, in such a way that the sum of the powers we choose must be n. This is the same as choosing a total of r items, when the items come in four distinct types (recall for example, Example 5.2). The types are represented by the factor the term is chosen from, and the exponent chosen from that factor is the number of items ($x$es) chosen of that type. So we know that the number of ways of doing this is $\left(\!\binom{4}{r}\!\right)$.

We have another way of working this out. Our generating function is $(1-x)^{-4}$, and the Generalised Binomial Theorem tells us that the coefficient of $(-x)^r$ in this is $\binom{-4}{r}$, so the coefficient of x^r is

$$(-1)^r(-1)^r\binom{r+3}{r} = \left(\!\!\binom{4}{r}\!\!\right).$$

We'll use the above example to work out a counting question, but first we need an observation.

PROPOSITION 7.13. *For any positive integer k,*

$$1+x+x^2+\cdots+x^k = \frac{1-x^{k+1}}{1-x}.$$

You can prove this by induction on k (this is one of the exercises below), or by multiplying through by $1-x$.

EXAMPLE 7.14. Trent is playing a dice game, using 12-sided dice. How many ways are there for him to roll a total of 24 on his four dice?

SOLUTION. Each die can roll any number between 1 and 12, and there are four dice, so the appropriate generating function is

$$(x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12})^4.$$

Rolling an i on one of the dice corresponds to choosing x^i from the corresponding factor of this generating function. We are looking for the coefficient of x^{24}, this will tell us the number of ways of rolling a total of 24.

It turns out that by manipulating the generating function, we can work this out a bit more easily than by multiplying this out. By taking a common factor of x out of each of the four factors, our generating function can be re-written as

$$x^4(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11})^4,$$

and the coefficient of x^{24} in this, will be the same as the coefficient of x^{20} in

$$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11})^4,$$

Using Proposition 7.13, we see that this expression can be rewritten as

$$\left(\frac{1-x^{12}}{1-x}\right)^4.$$

Using the Binomial Theorem and substituting $y = -x^{12}$, we see that

$$\begin{aligned}(1-x^{12})^4 &= \binom{4}{0}(-x^{12})^0 + \binom{4}{1}(-x^{12})^1 + \binom{4}{2}(-x^{12})^2 + \binom{4}{3}(-x^{12})^3 + \binom{4}{4}(-x^{12})^4 \\ &= 1 - 4x^{12} + 12x^{24} - 4x^{36} + x^{48}.\end{aligned}$$

Most of these terms can be ignored, as they will not contribute to the coefficient of x^{20}. Recall that the function we're interested in is the product of this, with $(1-x)^{-4}$, and there are only two ways of getting an x^{20} term from this product: by taking the constant term that we've just worked out, and multiplying it by the x^{20} term from $(1-x)^{-4}$; or by taking the x^{12} term that we've just worked out, and multiplying it by the x^8 term from $(1-x)^{-4}$. In the previous example, we worked out that in $(1-x)^{-4}$, the coefficient of x^{20} is $\left(\!\binom{4}{20}\!\right)$, and the coefficient of x^8 is $\left(\!\binom{4}{8}\!\right)$.

Thus, the number of ways in which Trent can roll a total of 24 on his four dice is the coefficient of x^{24} in our generating function, which is

$$\left(\!\!\binom{4}{20}\!\!\right) - 4\left(\!\!\binom{4}{8}\!\!\right) = 1771 - 660 = 1111. \qquad \square$$

EXERCISES 7.15.

1) Prove Proposition 7.13 by induction on k.
2) Find the number of ways Trent can roll a total of 16 on his four dice.
3) If Trent's four dice are 10-sided dice instead of 12-sided, how many ways can he roll a total of 24?
4) If Trent rolls five regular (6-sided) dice, how many ways can he roll a total of 11? What is the probability that he will roll a total of 11?

SUMMARY:

- If $n > 0$ is an integer, then
$$\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}.$$
- The Generalised Binomial Theorem
- $1 + x + \ldots + x^k = (1 - x^{k+1})/(1-x)$
- using generating functions for counting things
- Important definitions:
  - ○ generating function for a sequence
  - ○ generalised binomial coefficients

Chapter 8

Generating Functions and Recursion

We've seen how the Generalised Binomial Theorem can be used to extract coefficients from a certain sort of generating function. Before we proceed with learning how to use generating functions to find explicit formulas for the nth term of a recursively-defined sequence, we need to know how to extract coefficients from some more complicated expressions.

8A. Partial fractions

If a generating function looks like $1/(1+ax^i)^j$, we can use the Generalised Binomial Theorem to find the coefficient of x^r. But what can we do if the generating function looks like $1/(a+bx+cx^2)$, for example, or even more complicated expressions?

One tool that can help us extract coefficients from some expressions like this, is the method of partial fractions.

EXAMPLE 8.1. Suppose we have a generating function

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

How can we work out the coefficient of x^r?

SOLUTION. Well, if we could separate the factors of the denominator, we would know how to deal with each separately. In fact, this is exactly what we do. We set

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

As we work this through, you'll see that in working this out, we end up with two equations in the two unknowns A and B, which we can therefore solve! So it is possible to "split up" the original generating function, into two separate fractions, each of which has as its denominator one of the factors of the original denominator. This is the method of **partial fractions**.

To solve for A and B, we add the fractions $A/(1-2x)$ and $B/(2+x)$ over a common denominator. This gives

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

Clearly, this forces the numerators to be equal, so

$$A(2+x)+B(1-2x)=1+x.$$

Since these are equal as polynomials in x, the constant terms must be equal, and the coefficients of x must be equal, giving us two equations: $2A+B=1$ and $(A-2B)x=x$, so $A-2B=1$. Now there are many ways to algebraically solve for A and B; for example, the first equation gives $B=1-2A$; plugging this into the last equation gives $A-2(1-2A)=1$, so $5A=3$, so $A=3/5$. Now

$$B=1-2(3/5)=-1/5.$$

Thus, we have

$$f(x)=\frac{3/5}{1-2x}-\frac{1/5}{2+x}.$$

Notice that the $2+x$ is still a bit problematic. We can use the Generalised Binomial Theorem to work out coefficients for something that looks like $(1+ax^i)^j$, but we need that 1, and here instead we have a 2. To deal with this, we observe that

$$2+x=2(1+(1/2)x).$$

Thus,

$$f(x)=\frac{3/5}{1-2x}-\frac{1/10}{1+(1/2)x}.$$

Now let's expand each of the two summands separately. We have

$$\frac{3}{5}(1-2x)^{-1}=\frac{3}{5}(1+2x+(2x)^2+(2x)^3+\ldots),$$

so the coefficient of x^r in this part is $(3/5)2^r$. Also,

$$\frac{-1}{10}(1+(1/2)x)^{-1}=\frac{-1}{10}(1-\frac{1}{2}x+(\frac{1}{2}x)^2-(\frac{1}{2}x)^3+-\ldots),$$

so the coefficient of x^r in this part is $(-1/10)(-1)^r(1/2)^r$.

Thus, the coefficient of x^r in $f(x)$ is $(3/5)2^r-1/10(-1/2)^r$. □

The method of partial fractions can be applied to any generating function that has a denominator that can be factored into simpler terms. However, polynomials of degree 3 or higher can become hard to factor, so we'll mostly restrict our attention to applying this either with denominators that are already factored, or with denominators that have degree at most two.

There is an extra trick that you should be aware of. This arises if the denominator is divisible by a square. For example, if we are looking for the coefficient of x^r in

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

then it doesn't make sense to separate all of the factors out as before, because

$$g(x)=\frac{A}{1-2x}+\frac{B}{1-2x}+\frac{C}{2+x}=\frac{A+B}{1-2x}+\frac{C}{2+x}$$

and when we add this up, the denominator will be $(1-2x)(2+x)$ rather than $(1-2x)^2(2+x)$. This can be dealt with in either of two ways. First, you can include both $1-2x$ and $(1-2x)^2$ as denominators:

$$g(x)=\frac{A}{1-2x}+\frac{B}{(1-2x)^2}+\frac{C}{2+x}.$$

The second option is to include only $(1-2x)^2$ as one of the denominators, but to include an x in the corresponding numerator, in addition to the constant term:

$$g(x)=\frac{Ax+B}{(1-2x)^2}+\frac{C}{2+x}.$$

Either of these methods can be generalised in natural ways to cases where the denominator is divisible by some higher power.

We'll see more examples of partial fractions applied to specific situations, so we'll leave the explanation there for now.

EXERCISES 8.2. Find the coefficient of x^r in each of the following generating functions, using the method of partial fractions and the Generalised Binomial Theorem.

1) $\frac{1}{(1+2x)(2-x)}$
2) $\frac{x}{(1+x)^2(1-x)}$
3) $\frac{1+2x}{(1-2x)(2+x)(1+x)}$

8B. Factoring polynomials

You should be familiar with the quadratic formula, which allows us to factor any polynomial of degree two, into linear factors. Specifically, it tells us that the roots of ax^2+bx+c are

$$\frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

Notice that this does *not* tell us immediately how to factor ax^2+bx+c, because it's missing a constant factor of a. So if we want to factor ax^2+bx+c, we actually get

$$ax^2+bx+c = a\left(x-\left(\frac{-b+\sqrt{b^2-4ac}}{2a}\right)\right)\left(x-\left(\frac{-b-\sqrt{b^2-4ac}}{2a}\right)\right).$$

Recall that in order to use the Generalised Binomial Theorem, we need the constant term to be 1. If you are very comfortable with algebraic manipulations, you can use the quadratic formula to factor as above, and then divide each factor by the appropriate value so as to make the constant term 1. This may create a messy constant outside the whole thing, and a messy coefficient of x in each term, but if you are careful, you can get the correct answer this way.

If you are more confident in memorising another formula (closely related to the quadratic formula) for factoring ax^2+bx+c, you can also factor a quadratic polynomial directly into the form we want, using the following formula:

$$ax^2+bx+c = c\left(1-\frac{-b+\sqrt{b^2-4ac}}{2c}x\right)\left(1-\frac{-b-\sqrt{b^2-4ac}}{2c}x\right).$$

Sometimes a denominator will already be factored in the formula for a generating function, but when it isn't, either of the above methods can be used to factor it.

EXAMPLE 8.3. Factor $3x^2-2x+1$ into linear factors.

SOLUTION. We will use the formula given above. We have $a=3$, $b=-2$, and $c=1$. Then

$$\begin{aligned} 3x^2-2x+1 &= \left(1-\frac{2+\sqrt{4-12}}{2}x\right)\left(1-\frac{2-\sqrt{4-12}}{2}x\right) \\ &= (1-(1+i\sqrt{2})x)(1-(1-i\sqrt{2})x). \end{aligned}$$

□

It is always a good idea to check your result, by multiplying the factors back out.

When coefficients in the factorisation get ugly (even complex, as in the example above), you might find the algebra involved in working out the coefficients hard to deal with. Let's work through an example of this, using the factorisation we've just completed.

EXAMPLE 8.4. Find the coefficient of x^r in $f(x)$, where

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

SOLUTION. We have determined in the previous example, that

$$3x^2 - 2x + 1 = (1 - (1 + i\sqrt{2})x)(1 - (1 - i\sqrt{2})x),$$

so we need to solve for A and B, where

$$\begin{aligned} f(x) &= \frac{1}{3x^2 - 2x + 1} \\ &= \frac{A}{1 - (1 + i\sqrt{2})x} + \frac{B}{1 - (1 - i\sqrt{2})x} \\ &= \frac{A(1 - (1 - i\sqrt{2})x) + B(1 - (1 + i\sqrt{2})x)}{3x^2 - 2x + 1}. \end{aligned}$$

Thus,

$$A(1 - (1 - i\sqrt{2})x) + B(1 - (1 + i\sqrt{2})x) = 1 + 0x,$$

so the constant term gives $A + B = 1$, while the coefficient of x gives $A(1 - i\sqrt{2}) + B(1 + i\sqrt{2}) = 0$. Substituting $B = 1 - A$ into the latter equation, gives

$$A - i\sqrt{2}A + 1 + i\sqrt{2} - A - i\sqrt{2}A = 0,$$

so $1 + i\sqrt{2} = i2\sqrt{2}A$. Hence

$$A = \frac{1 + i\sqrt{2}}{i2\sqrt{2}} = \frac{1}{2\sqrt{2}i} + \frac{1}{2}.$$

We make the denominator of the first fraction rational, by multiplying numerator and denominator by $\sqrt{2}i$, giving

$$A = -\frac{\sqrt{2}i}{4} + \frac{1}{2}.$$

Now since $B = 1 - A$, we have

$$B = \frac{1}{2} + \frac{\sqrt{2}i}{4}.$$

To make things a bit simpler, we'll rewrite A as $(2 - \sqrt{2}i)/4$, and $B = (2 + \sqrt{2}i)/4$.

Thus we have

$$f(x) = \frac{(2 - \sqrt{2}i)/4}{1 - (1 + i\sqrt{2})x} + \frac{(2 + \sqrt{2}i)/4}{1 - (1 - i\sqrt{2})x}.$$

Using the Generalised Binomial Theorem and $y = (1 + i\sqrt{2})x$, we see that the first fraction expands as

$$[(2 - \sqrt{2}i)/4](1 + y + y^2 + y^3 + \ldots),$$

and the coefficient of x^r in this, will be $[(2 - \sqrt{2}i)/4](1 + i\sqrt{2})^r$. Similarly, with $y = (1 - i\sqrt{2})x$, the second fraction expands as

$$[(2 + \sqrt{2}i)/4](1 + y + y^2 + y^3 + \ldots),$$

and the coefficient of x^r in this, will be $[(2 + \sqrt{2}i)/4](1 - i\sqrt{2})^r$.

So the coefficient of x^r in $f(x)$ is

$$[(2 - \sqrt{2}i)/4](1 + i\sqrt{2})^r + [(2 + \sqrt{2}i)/4](1 - i\sqrt{2})^r. \qquad \square$$

You can see from this example that the algebra can get ugly, but the process of finding the coefficient of x^r is nonetheless straightforward.

EXERCISES 8.5. For each of the generating functions given, factor the denominator and use the method of partial fractions to determine the coefficient of x^r.

1) $\frac{x}{x^2+5x-1}$

2) $\frac{2+x}{2x^2+x-1}$

3) $\frac{x}{x^2-3x+1}$

8C. Using generating functions to solve recursively-defined sequences

At last we are ready to apply the mechanics we've introduced in this chapter, to find an explicit formula for the nth term of a recursively-defined sequence.

This method is probably most easily understood using examples.

EXAMPLE 8.6. Consider the recursively-defined sequence: $a_0 = 2$, and for every $n \geq 1$, $a_n = 3a_{n-1} - 1$. Find an explicit formula for a_n in terms of n.

SOLUTION. The generating function for this sequence is $a(x) = \sum_{i=0}^{\infty} a_i x^i$.

Now, we are going to use the recursive relation. We know that $a_n = 3a_{n-1} - 1$, or, by rearranging this, $a_n - 3a_{n-1} = -1$. Thus, if we could get the coefficient of x^n to look like $a_n - 3a_{n-1}$, we could use the recursive relation to replace this by -1. Right now, the coefficient of x^n is a_n, and the only place a_{n-1} shows up is as the coefficient of x^{n-1}. But if we multiply $a(x)$ by x, then $a_{n-1}x^{n-1}$ becomes $a_{n-1}x^n$, so if we also multiply by -3, we get a coefficient of $-3a_{n-1}$ for x^n in $-3xa(x)$. Now add this to $a(x)$. This may be easier to see as written below:

$$\begin{array}{ccccccccc} a(x) & = & a_0 & +a_1x & +a_2x^2 & +\ldots & +a_mx^m & +\ldots \\ -3xa(x) & = & & -3a_0x & -3a_1x^2 & -\ldots & -3a_{m-1}x^m & -\ldots \\ \hline (1-3x)a(x) & = & a_0 & -x & -x^2 & -\ldots & -x^m & -\ldots \end{array}$$

We see that this gives

$$(1-3x)a(x) = 3 - (1 + x + x^2 + x^3 + \ldots),$$

and we know that

$$1 + x + x^2 + x^3 + \ldots = 1/(1-x),$$

so $(1-3x)a(x) = 3 - 1/(1-x)$. Dividing through by $1-3x$ gives

$$a(x) = \frac{3}{1-3x} - \frac{1}{(1-x)(1-3x)}.$$

Now it's time to apply what we learned in the preceding sections of this chapter. The denominator is already factored, so we can immediately apply the method of partial fractions to the second fraction. If

$$\frac{-1}{(1-x)(1-3x)} = \frac{A}{1-x} + \frac{B}{1-3x} = \frac{A(1-3x) + B(1-x)}{(1-3x)(1-x)},$$

then $A + B = -1$ and $-3A - B = 0$, so $B = -3A$, which gives $-2A = -1$, so $A = 1/2$ and $B = -3/2$. Thus,

$$a(x) = \frac{3}{1-3x} + \frac{1/2}{1-x} - \frac{3/2}{1-3x} = \frac{1/2}{1-x} + \frac{3/2}{1-3x}.$$

The coefficient of x^n in the first of these terms is $1/2$, while in the second term, the coefficient of x^n is $(3/2)3^n$. Thus, $a_n = 1/2 + (3/2)3^n$. Since our generating function began with a_0x^0, this formula applies for every $n \geq 0$.

When going through so much algebra, it's easy to make a mistake somewhere along the way, so it's wise to do some double-checking. For a recursively-defined sequence, if the formula you work out gives the correct answer for the first three or four terms of the sequence, then it's very likely that you've done the calculations correctly. Let's check the first three terms of this one. We know from our initial condition that $a_0 = 2$, and our new formula gives

$$a_0 = 1/2 + (3/2)3^0 = 1/2 + 3/2 = 2.$$

Using the recursive relation, we should have $a_1 = 3(2) - 1 = 5$, and our formula gives

$$a_1 = 1/2 + (3/2)3^1 = 1/2 = 9/2 = 5.$$

Finally, the recursive relation gives $a_2 = 3(5) - 1 = 14$, while our formula gives

$$a_2 = 1/2 + (3/2)3^2 = 1/2 + 27/2 = 14.$$

You can see the benefit to having an explicit formula if you were asked to work out a_{100}. Clearly, it's much easier to determine $1/2 + (3/2)3^{100}$ than to apply the recursive relation one hundred times. □

Let's look at one more example, where the recursive relation involves more than one previous term.

EXAMPLE 8.7. Consider the recursively-defined sequence: $b_0 = 1$, $b_1 = 0$, $b_2 = 1$, and for every $n \geq 3$, $b_n = b_{n-1} - 2b_{n-3}$. Find an explicit formula for b_n in terms of n.

SOLUTION. The generating function for this sequence is

$$b(x) = \sum_{i=0}^{\infty} b_i x^i.$$

Again, we'll use the recursive relation, which we rearrange as

$$b_n - b_{n-1} + 2b_{n-3} = 0$$

for every $n \geq 3$. We want to end up with a polynomial in which the coefficient of x^m looks like $b_m - b_{m-1} + 2b_{m-3}$, so that we'll be able to use the recursive relation to replace this by 0. In order to do this, we'll take $b(x)$ (to get the $b_m x^m$ piece), minus $xb(x)$ (to get the $-b_{m-1}x^m$ piece), plus $2x^3b(x)$ (to get the $+2b_{m-3}x^m$ piece).

The result looks like:

$$\begin{array}{rcccccccc}
b(x) & = & b_0 & +b_1x & +b_2x^2 & +b_3x^3 & +\ldots & +b_mx^m & +\ldots \\
-xb(x) & = & & -b_0x & -b_1x^2 & -b_2x^3 & -\ldots & -b_{m-1}x^m & -\ldots \\
+2x^3b(x) & = & & & & +2b_0x^3 & +\ldots & +2b_{m-3}x^m & +\ldots \\
\hline
(1-x+2x^3)b(x) & = & b_0 & +(b_1-b_0)x & +(b_2-b_1)x^2 & +0x^3 & +\ldots & +0x^m & +\ldots
\end{array}$$

We see that this gives

$$(1 - x + 2x^3)b(x) = 1 + (-1)x + 1x^2.$$

Dividing through by $1 - x + 2x^3$ gives

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

If we want to be able to do anything with this, we need to factor the denominator. Although we don't have a general method for factoring cubic polynomials, in this case it's not hard to see that -1 is a zero of the polynomial (because $1 - (-1) + 2(-1)^3 = 0$), and hence $x + 1$ is a factor of the polynomial. You will not be expected to factor cubic polynomials yourself in this course, so we won't review polynomial long division, but if you recall polynomial long division, you can use it to determine that

$$1 - x + 2x^3 = (1 + x)(2x^2 - 2x + 1).$$

In any case, you can multiply the right-hand side out to verify that it is true.

Now it's time to use the factoring formula, with $a = 2$, $b = -2$, and $c = 1$, to factor $2x^2 - 2x + 1$. This gives

$$2x^2 - 2x + 1 = 1\left(1 - \frac{2+\sqrt{4-8}}{2}x\right)\left(1 - \frac{2-\sqrt{4-8}}{2}x\right) = (1-(1+i)x)\,(1-(1-i)x)\,.$$

Having factored

$$1 - x + 2x^3 = (1+x)(1-(1+i)x)(1-(1-i)x),$$

we now apply the method of partial fractions to split this up into three separate pieces.

If

$$\begin{aligned}\frac{1-x+x^2}{1-x+2x^3} &= \frac{A}{1+x} + \frac{B}{1-(1+i)x} + \frac{C}{1-(1-i)x}\\ &= \frac{A(2x^2-2x+1) + B(1+x)(1-(1-i)x) + C(1+x)(1-(1+i)x)}{1-x+2x^3},\end{aligned}$$

then this gives us three equations:

$$2A - B(1-i) - C(1+i) = 1$$

(from the coefficient of x^2);

$$-2A + B(1-(1-i)) + C(1-(1+i)) = -1$$

(from the coefficient of x); and $A + B + C = 1$ (from the constant term). The second of these simplifies to $-2A + iB - iC = -1$.

The algebra can be done in different ways and gets a bit ugly, but these three equations can be solved, resulting in $A = 3/5$, $B = (2-i)/10$, $C = (2+i)/10$.

Thus,

$$\frac{1-x+x^2}{1-x+2x^3} = \frac{3/5}{1+x} + \frac{(2-i)/10}{1-(1+i)x} + \frac{(2+i)/10}{1-(1-i)x}.$$

The coefficient of x^n in the first of these terms is $(3/5)(-1)^n$; in the second, it is $((2-i)/10))(1+i)^n$, and in the third, it is $((2+i)/10)(1-i)^n$.

We conclude that for every $n \geq 0$, we have

$$b_n = \frac{3}{5}(-1)^n + \frac{2-i}{10}\,(1+i)^n + \frac{2+i}{10}\,(1-i)^n\,.$$

It is somewhat surprising that these formulas involving complex numbers will always work out (when n is an integer) to be not only real numbers, but integers! Once again, we should check this formula for several values of n to ensure we haven't made errors in our calculations along the way.

From the initial conditions, $b_0 = 1$. Our formula gives

$$b_0 = 3/5 + (2-i)/10 + (2+i)/10 = 1.$$

From the initial conditions, $b_1 = 0$. Our formula gives

$$b_1 = -3/5 + \frac{2-i}{10}(1+i) + \frac{2+i}{10}(1-i) = -3/5 + (3+i)/10 + (3-i)/10 = 0.$$

Finally, the initial conditions gave $b_2 = 1$, and our formula gives

$$b_2 = \frac{3}{5} + \frac{2-i}{10}(2i) + \frac{2+i}{10}(-2i) = \frac{3}{5} + \frac{2i+1}{5} - \frac{2i-1}{5} = 1.$$

We could continue, but this is sufficient verification to inspire reasonable confidence. □

We now have a general method that we can apply to solve normal linear recursive relations:
Method

1) Rearrange the recurrence relation into the form
$$h_n - a_1h_{n-1} - a_2h_{n-2} - \ldots - a_kh_{n-k} = f(n),$$
for some function $f(n)$. Let
$$a(x) = 1 - a_1x - a_2x^2 - \ldots - a_kx^k.$$

2) Define the generating function
$$h(x) = h_0 + h_1x + h_2x^2 + \ldots.$$

3) Find a linear combination of the generating function so that the coefficient of x^m is $f(m)$ for every m greater than or equal to some $i \geq k$:

$$\begin{array}{rclllllll}
h(x) & = & h_0 & +h_1x & +h_2x^2 & +h_3x^3 & +\ldots & +h_ix^i & +\ldots \\
-a_1xh(x) & = & & -a_1h_0x & -a_1h_1x^2 & -a_1h_2x^3 & -\ldots & -a_1h_{i-1}x^i & -\ldots \\
-a_2x^2h(x) & = & & & -a_2h_0x^2 & -a_2h_1x^3 & -\ldots & -a_2h_{i-2}x^i & +\ldots \\
\vdots & & & & & & & \vdots & \\
-a_kx^kh(x) & = & & & & & & -a_kh_{i-k}x^i & +\ldots \\
\hline
a(x)h(x) & = & h_0 & +(h_1-a_1h_0)x & +(h_2-a_1h_1-a_2h_0)x^2 & +\ldots & \ldots & +f(i)x^i & +\ldots
\end{array}$$

So
$$h(x) = \frac{h_0 + (h_1 - a_1h_0)x + \ldots + (h_{i-1} - a_1h_{i-2} + \ldots + a_{k-1}h_{i-k})x^{i-1} + \sum_{n=i}^{\infty} f(n)x^n}{a(x)}.$$

4) Factor $a(x)$ (remember that you can use complex roots), and find a closed form for
$$\sum_{n=i}^{\infty} f(n)x^n.$$

5) Use partial fractions to get expressions that we can expand using the generalised binomial theorem.

6) Make variable substitutions if necessary to get forms that look like
$$\frac{A}{(1+y)^n}.$$

7) Use the generalised binomial theorem to find h_n, the coefficient of x^n in $h(x)$.

EXERCISES 8.8. For each of the following recursively-defined sequences, use the method of generating functions to find an explicit formula for the nth term of the sequence.

1) $c_0 = 2$, $c_1 = 0$, $c_n = c_{n-1} + 2c_{n-2}$ for every $n \geq 2$.
2) $d_0 = 0$, $d_1 = 1$, $d_n = 2d_{n-2} + 1$ for every $n \geq 2$.
3) $e_0 = 2$, $e_n = 3e_{n-1} - 2$ for every $n \geq 1$.
4) $f_0 = 1$, $f_1 = 3$, and $f_n = 4(f_{n-1} - f_{n-2})$ for every $n \geq 2$.
5) $g_0 = 2$, $g_1 = 0$, and $g_n = 2g_{n-1} - 2g_{n-2}$ for every $n \geq 2$.
6) $h_0 = 1/2$ and $h_n = 3h_{n-1} - 1/2$ for every $n \geq 1$.
7) $i_0 = i_1 = 2$, $i_2 = 0$, and $i_n = 3i_{n-1} - 3i_{n-2} + i_{n-3}$ for every $n \geq 3$.
8) $j_0 = -1$, $j_1 = 0$, and $j_n = 2j_{n-1} + 3j_{n-2}$ for every $n \geq 2$.
9) $k_0 = 10$ and $k_n = 11k_{n-1} - 10$ for every $n \geq 1$.

EXERCISES 8.9. Solve the following problems.

1) Let p_n denote the number of ways to build a pipe n units long, using segments that are either plastic or metal, and (for each material) come in lengths of 1 unit or 2 units. For example, $p_1 = 2$ since we can use a 1-unit segment that is either plastic or metal, and $p_2 = 6$ since we can use either type of 2-unit segment, or any of the 2^2 possible ordered choices of 2 segments each having a length of 1 unit. Define $p_0 = 1$.

   Determine a recurrence relation for p_n. Give a combinatorial proof that your recurrence relation does solve this counting problem. Use your recurrence relation and the method of generating functions to find a formula for p_n.

   [*Hint:* Your final answer should be
$$p_n = \frac{1}{2\sqrt{3}}(1+\sqrt{3})^{n+1} - \frac{1}{2\sqrt{3}}(1-\sqrt{3})^{n+1}$$
   for every $n \geq 0$.]

2) Let s_n denote the number of lists of any length that have the fixed sum of n, and whose entries come from $\{1, 2, 3\}$. For example, $s_2 = 2$ because $(1, 1)$ and (2) are the only such lists; and $s_4 = 7$ because the lists are $(3, 1)$, $(1, 3)$, $(2, 2)$, $(2, 1, 1)$, $(1, 2, 1)$, $(1, 1, 2)$, and $(1, 1, 1, 1)$. Define $s_0 = 1$.

   Determine s_1, s_3, and s_5 by finding all possible lists. Give a combinatorial proof that $s_n = s_{n-1} + s_{n-2} + s_{n-3}$ for every $n \geq 3$. Use this recurrence relation to show that the generating function $S(x)$ for $\{s_n\}$ is $\frac{1}{1-x-x^2-x^3}$.

SUMMARY:

- Method of partial fractions
- Formula for factoring quadratic polynomials into the required form
- Applying generating functions to recursively-defined sequences

Chapter 9

Some Important Recursively-Defined Sequences

9A. Derangements

DEFINITION 9.1. A **derangement** of a list of objects, is a permutation of the objects, in which no object is left in its original position.

A classic example of this is a situation in which you write letters to ten people, address envelopes to each of them, and then put them in the envelopes, but accidentally end up with none of the letters in the correct envelope.

Another example might be a dance class in which five brother-sister pairs are enrolled. The instructor mixes them up so that no one is dancing with a sibling.

Since we're considering enumeration, it shouldn't surprise you that the question we want answered is: in how many ways can this happen? That is, given n objects, how many derangements of the n objects are there? Let's use D_n to denote the number of derangements of n objects.

We can label the objects with the numbers $\{1, \ldots, n\}$, and think of a derangement as a bijection

$$f : \{1, \ldots, n\} \to \{1, \ldots, n\},$$

such that f does not fix any value. There are $n-1$ choices for $f(n)$, since the only restriction is $f(n) \neq n$. Say $f(n) = i$. We consider two possible cases.

Case 1 $\boldsymbol{f(i) = n}$. Now, on the other $n-2$ values between 1 and n that are neither i nor n, f must map $\{1, \ldots, n-1\} \setminus \{i\}$ to $\{1, \ldots, n-1\} \setminus \{i\}$, and must be a derangement. So there are D_{n-2} derangements that have $f(n) = i$ and $f(i) = n$.

Case 2 $\boldsymbol{f(j) = n}$ for some $\boldsymbol{j \neq i}$. In this case, we define another function

$$g : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$$

as follows. We set $g(j) = i$, and for every other value, $g(a) = f(a)$ (that is, for every $a \in \{1, \ldots, n-1\} \setminus \{j\}$). We had $f(j) = n$ and $f(n) = i$, and we are eliminating n from the derangement while maintaining a bijection, by creating the shortcut f with $g(j) = i$ but $g(a) = f(a)$ for every other $a \in \{1, \ldots, n-1\}$. Since f is a derangement and $j \neq i$, we see that g is also a derangement (this time of $n-1$ objects). So there are D_{n-1} possible derangements g, and for a fixed choice of i, these are in one-to-one correspondence with derangements f that have $f(j) = n$ and $f(n) = i$, so there are also D_{n-1} of these.

We conclude that $D_n = (n-1)(D_{n-1} + D_{n-2})$.

We also need some initial conditions. We have $D_1 = 0$; there is no way of arranging a single object so that it doesn't end up in the correct place. Also, $D_2 = 1$, since there is exactly one way of deranging two objects (by interchanging them).

If we wanted to solve this recursively-defined sequence, we would need to use *exponential generating functions*, which we'll introduce in this chapter but won't really study in this course. Instead, we'll give the explicit formula for D_n without proof.

PROPOSITION 9.2. *For any $n \geq 1$, the number of derangements of n objects is*

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

EXERCISES 9.3.

1) Use induction to prove Proposition 9.2.

2) Which kind of induction did you have to use to prove Proposition 9.2?

3) Calculate D_5 using the explicit formula given in Proposition 9.2.

4) Calculate D_5 using the recursive relation.

9B. Catalan numbers

This is an example that shows even more clearly the power of the generating function method.

The Catalan numbers are a sequence that can be defined in a variety of ways, because they arise in a number of different circumstances. We'll use the following definition.

DEFINITION 9.4. The nth **Catalan number**, C_n, is the number of different ways in which brackets can be put around n terms, to indicate different orders of combining the terms.

Thus, for example, $C_3 = 2$, since three terms can be combined as either

$$[(\_ \cdot \_) \cdot \_], \text{ or } [\_ \cdot (\_ \cdot \_)].$$

These numbers have something in common with Example 6.15, in which Shawna was building towers from lego. If we'd asked in how many different orders she could combine the blocks to build her tower, assuming that the final order for the blocks was decided in advance, we would have been asking for the Catalan number. So we can use logic similar to the logic we used in that example: in order to create an expression with n terms, our final step must involve combining a set of k terms (for which the order of combining them has already been determined) and a set of $n-k$ terms (for which the order of combining them has already been determined). Here, k may take on any value from 1 to $n-1$. This results in the recursive relation:

$$C_n = \sum_{k=1}^{n-1} C_k C_{n-k}.$$

This may be easier to see with an example. We've worked out C_3 above; in order to work out C_4 using this recursive relation, we also need to know C_1 and C_2. There is only one way to combine a single term (we don't need brackets at all), so $C_1 = 1$. We also have $C_2 = 1$, since there is only one way to put brackets around a pair of terms: $(\_ \cdot \_)$.

Now, to use brackets to order the operations in a four-term expression, our final operation must either combine a group of three terms with a single term; a group of two terms with another group of two terms; or a single term with a group of three terms (this time, the single term is at the left). The first two expressions below come from combining a group of three terms with a single term; the third comes from combining a group of two terms with another group of two terms; and the last two come from combining a single term with a group of three terms.

$$([(\_\cdot\_)\cdot\_]\cdot\_),\qquad ([\_\cdot(\_\cdot\_)]\cdot\_),\qquad [(\_\cdot\_)\cdot(\_\cdot\_)]\qquad (\_\cdot[(\_\cdot\_)\cdot\_])\qquad (\_\cdot[\_\cdot(\_\cdot\_)]).$$

Thus,

$$C_4 = C_3C_1 + C_2C_2 + C_1C_3 = 2 + 1 + 2 = 5.$$

Now we want to use generating functions to figure out what we can about the Catalan numbers. Unfortunately, there is a difficulty. Any time we want to use generating functions to solve a recursively-defined sequence, the sequence must start with a 0th term, to be the coefficient of x^0. With some recursively-defined sequences, we can simply use the recursive relation "backwards" to solve previous terms, going down to $n = 0$, even if our initial conditions began with much higher terms. For example, if a recursively-defined sequence is given by $h_2 = 1, h_3 = 5$ and $h_n = 8h_{n-2} - h_{n-1}$ for every $n \geq 4$, we can use $n = 3$ in this to get

$$h_3 = 5 = 8h_1 - h_2 = 8h_1 - 1.$$

Solving for h_1 gives $h_1 = 3/4$. Then using the recursive relation with $n = 2$ gives

$$h_2 = 1 = 8h_0 - h_1 = 8h_0 - 3/4.$$

Solving for h_0 gives $h_0 = 7/32$. This allows us to use generating functions on the sequence.

The recursive relation for the Catalan numbers doesn't have a form that allows us to solve for C_0 by knowing other terms of the sequence, so we do what we have to, in order to make things work. Instead of working with the generating function for the Catalan numbers themselves (since we can't), we work with the generating function for the sequence $c_0, c_1, c_2, \ldots$, where $c_i = C_{i+1}$ for every $i \geq 0$. In other words, the nth term of our new sequence will be the $n+1$st Catalan number.

Adjusting the recursive relation we've determined for the Catalan numbers to this new sequence, gives

$$c_0 = 1, \text{ and } c_n = \sum_{k=0}^{n-1} c_k c_{n-k-1} \text{ for every } n \geq 1.$$

Notice that

$$\begin{aligned} c(x)c(x) &= (c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots)(c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots) \\ &= c_0c_0 + (c_1c_0 + c_0c_1)x + (c_2c_0 + c_1c_1 + c_0c_2)x^2 + (c_0c_3 + c_1c_2 + c_2c_1 + c_3c_0)x^3 + \ldots \end{aligned}$$

and in general, the coefficient of x^m in $(c(x))^2$, is

$$\sum_{k=0}^{m} c_k c_{m-k}.$$

This should look familiar! In fact, you can see that the coefficient of x^m in $(c(x))^2$, is the same as the coefficient of x^{m+1} in $c(x)$, since the latter is

$$\sum_{k=0}^{m} c_k c_{m-k}$$

also.

Thus, we have an expression for $c(x)$ in terms of $(c(x))^2$, since multiplying $(c(x))^2$ by x gives all of the terms of $c(x)$ except c_0: $c(x) = x(c(x))^2 + c_0$. We can rearrange this equation, to see that

$$x[c(x)]^2 - c(x) + 1 = 0.$$

We are about to do something to this generating function that may seem a bit like black magic: we will use the quadratic formula to factor this quadratic equation in $c(x)$, treating x as the coefficient of $(c(x))^2$. Thus, in the quadratic formula, we take $a = x$, $b = -1$, and $c = 1$, and obtain

$$c(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Of course, there are two roots to this, and only one of them will give the correct generating function; we need to work out which one (whether to take the plus or the minus).

Using the Generalised Binomial Theorem, we see that

$$(1-4x)^{1/2} = \binom{1/2}{0} + \binom{1/2}{1}(-4x) + \binom{1/2}{2}(-4x)^2 + \ldots + \binom{1/2}{k}(-4x)^k + \ldots,$$

and

$$\binom{1/2}{k} = \frac{(1/2)(-1/2)(-3/2)\ldots(1/2-k+1)}{k!} = \frac{(-1)^{k-1}1\cdot 3\cdot 5\cdot(2k-3)}{2^k k!}$$

so the coefficient of x^k in $(1-4x)^{1/2}$ is

$$\frac{(-1)^{k-1}1\cdot 3\cdot 5\cdot(2k-3)}{2^k k!}(-4)^k = \frac{(-1)1\cdot 3\cdot 5\cdot(2k-3)2^k}{k!}.$$

Whichever root we use will require this expression, so let's work with it a bit more to get it into a nicer form.

$$2^k k! = 2^k(1\cdot 2\cdot 3\cdot\ldots\cdot k) = 2\cdot 4\cdot 6\cdot\ldots\cdot 2k,$$

so if we multiply the numerator and denominator of the fraction by $k!$ (which does not change the result), we see that we have

$$\frac{(-1)1\cdot 3\cdot 5\cdot(2k-3)2\cdot 4\cdot 6\ldots\cdot 2k}{k!k!} = \frac{(-1)(2k-2)!2k}{k!k!} = \frac{(-1)(2k)!}{(2k-1)k!k!} = \frac{-1}{2k-1}\binom{2k}{k},$$

so

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

The coefficients shown on the right-hand side of this equation quickly get big and negative. If

$$c(x) = \frac{1+\sqrt{1-4x}}{2x},$$

then for $n > 0$ the coefficient of x^n in $c(x)$ will be half of the coefficient of x^{n+1} in $(1-4x)^{1/2}$, which (when n is large) will be big and negative. But it is easy to see from the recurrence relation that all of the Catalan numbers are positive. To get positive coefficients, we must use

$$c(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

Since in this expression we take the negative of the large negative coefficients, the result will be large positive coefficients (even when we divide by 2, and look for the coefficient of x^{n+1}).

Thus,

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

From this, we see that for $n > 0$, the coefficient of x^n in $c(x)$ is half of the coefficient of x^{n+1} in $(1-4x)^{1/2}$, which is

$$\begin{aligned}\frac{1}{2}\binom{2(n+1)}{n+1}\frac{1}{2n+1} &= \frac{(2n+2)!}{2(n+1)!(n+1)!(2n+1)}\\ &= \frac{1}{2}\cdot\frac{2n+2}{n+1}\cdot\frac{(2n)!}{(n+1)!n!}\cdot\frac{2n+1}{2n+1}\\ &= \frac{1}{n+1}\binom{2n}{n}.\end{aligned}$$

So

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

Although we derived this expression for $n > 0$ only, we can verify that $c_0 = 1 = \frac{1}{0+1}\binom{0}{0}$ since $0! = 1$, so this expression is true for every $n \geq 0$.

EXERCISES 9.5.

1) Use induction and the recursive relation for Catalan numbers (as adjusted for the values of $\{c_i\}$, where $c_i = C_{i+1}$) to prove that $c_n > 0$ for every $n \geq 0$.
2) Calculate c_4 using the explicit formula that we calculated in this section.
3) Calculate c_4 using the recursive relation.

9C. Bell numbers and exponential generating functions

Sometimes a recurrence relation involves factorials, or binomial coefficients. When this happens, it becomes difficult if not impossible to use ordinary generating functions to find an explicit formula for the nth term of the sequence. In some cases, a different kind of generating function, the exponential generating function, may succeed where an ordinary generating function fails.

DEFINITION 9.6. The **exponential generating function** for the sequence $a_0, a_1, \ldots$, is

$$\sum_{i=0}^{\infty}\frac{a_i x^i}{i!}.$$

Obviously, the difference between this and an ordinary generating function comes from the factorial expression in the denominator. Cancellation between this and expressions in the numerator can lead to nicer compact expressions.

EXAMPLE 9.7. The exponential generating function for the sequence $1, 1, 1, \ldots$ is

$$\frac{1}{0!}+\frac{x}{1!}+\frac{x^2}{2!}+\ldots.$$

This is the Taylor series expansion for e^x. Thus, e^x is the exponential generating function for $1, 1, 1, \ldots$.

We will not be using exponential generating functions in this class; we are just introducing the topic. We will go through one example of a sequence for which exponential generating functions are useful: the Bell numbers.

DEFINITION 9.8. The **Bell number** B_n is the number of partitions of $\{1, \ldots, n\}$ into subsets.

Let's look at the first few Bell numbers.

EXAMPLE 9.9. There is only one way to partition $\{1\}$ into subsets: $\{1\}$, so $B_1 = 1$.

There are two ways to partition $\{1, 2\}$ into subsets: $\{1\}, \{2\}$, or $\{1, 2\}$, so $B_2 = 2$.

There are five ways to partition $\{1, 2, 3\}$ into subsets: $\{1\}, \{2\}, \{3\}$, or $\{1, 2\}, \{3\}$, or $\{1, 3\}, \{2\}$, or $\{2, 3\}, \{1\}$, or $\{1, 2, 3\}$, so $B_3 = 5$.

Probably after seeing the above examples, you don't want to calculate larger Bell numbers directly. However, we can derive a recursive relation for these numbers. For this relation to work properly, we will define $B_0 = 1$.

PROPOSITION 9.10. *For $n \geq 1$, the nth Bell number*

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}.$$

PROOF. We'll use a combinatorial proof of this statement. We know that B_n is the number of partitions of $\{1, \ldots, n\}$ into subsets.

For the other side of the equation, let's consider the subset that contains the element n, and call the cardinality of this subset k. Since n is in this subset, $k \geq 1$, and since this is a subset of $\{1, \ldots, n\}$, we have $k \leq n$, so $1 \leq k \leq n$. There are $\binom{n-1}{k-1}$ ways to choose the remaining $k-1$ elements of this subset; that is, for any $1 \leq k \leq n$, there are $\binom{n-1}{k-1}$ ways to choose the subset of $\{1, \ldots n\}$ that contains the element n. For each of these ways, there are $n - k$ other elements that must be partitioned, and by the definition of the Bell numbers, there are B_{n-k} ways to partition them into subsets. (Our definition of $B_0 = 1$ deals with the case $k = n$, ensuring that the $\binom{n-1}{n-1} = 1$ way of choosing n to be in a single set of all n elements is counted once and only once.)

Thus, using the product and sum rules, we see that

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}. \qquad \square$$

Let us try to find the exponential generating function for the Bell numbers. When dealing with exponential generating functions, notice that the derivative of $x^n/n!$ is $nx^{n-1}/n! = x^{n-1}/(n-1)!$, so taking derivatives often results in a nice expression that helps us find a nice expression for the coefficients. You already know a particularly nice example of this: the derivative of e^x is e^x, which tells us that all of the coefficients in that exponential generating function are equal.

Define

$$B(x) = \sum_{i=0}^{\infty} B_i \frac{x^i}{i!} = B_0 + B_1 \frac{x}{1!} + B_2 \frac{x^2}{2!} + \ldots + B_n \frac{x^n}{n!} + \ldots.$$

Notice that the derivative of this is

$$\begin{aligned} \frac{d}{dx} B(x) &= B_1 + B_2 \frac{x}{1!} + B_3 \frac{x^2}{2!} + \ldots + B_n \frac{x^{n-1}}{(n-1)!} + \ldots \\ &= \sum_{n=1}^{\infty} B_n \frac{x^{n-1}}{(n-1)!}. \end{aligned}$$

Using our recursive relation from Proposition 9.10, we see that this is

$$\begin{aligned}\frac{d}{dx}B(x) &= \sum_{n=1}^{\infty}\left[\sum_{k=1}^{n}\binom{n-1}{k-1}B_{n-k}\right]\frac{x^{n-1}}{(n-1)!}\\ &= \sum_{n=1}^{\infty}\left[\sum_{k=1}^{n}\frac{(n-1)!}{(k-1)!(n-k)!}B_{n-k}\frac{x^{n-1}}{(n-1)!}\right]\\ &= \sum_{n=1}^{\infty}\left[\sum_{k=1}^{n}\frac{1}{(k-1)!(n-k)!}B_{n-k}x^{n-1}\right]\\ &= \sum_{n=1}^{\infty}\left[\sum_{k=1}^{n}\frac{x^{k-1}}{(k-1)!}B_{n-k}\frac{x^{n-k}}{(n-k)!}\right].\end{aligned}$$

Notice that for each value of n, as k goes from 1 to n the values $k-1$ and $n-k$ take on every pair of non-negative integral values that add up to n. Thus, as n goes from 1 to infinity, the values $k-1$ and $n-k$ take on every possible pair of non-negative integral values. Therefore, we can rewrite this expression as

$$\begin{aligned}\frac{d}{dx}B(x) &= \sum_{j=0}^{\infty}\left[\sum_{i=0}^{\infty}\frac{x^j}{j!}B_i\frac{x^i}{i!}\right]\\ &= \sum_{j=0}^{\infty}\frac{x^j}{j!}\left[\sum_{i=0}^{\infty}B_i\frac{x^i}{i!}\right]\\ &= \left[\sum_{j=0}^{\infty}\frac{x^j}{j!}\right]\left[\sum_{i=0}^{\infty}B_i\frac{x^i}{i!}\right]\\ &= e^xB(x).\end{aligned}$$

Now, consider the derivative of $e^{-(e^x)}B(x)$. By the product and chain rules, this is

$$e^{-(e^x)}e^xB(x) - B(x)e^{-(e^x)}e^x = 0,$$

so it must be the case that $e^{-(e^x)}B(x)$ is constant, say $e^{-(e^x)}B(x) = c$. Then $B(x) = ce^{(e^x)}$.

Since

$$B(0) = \sum_{n=0}^{\infty}B_n\frac{0^n}{n!} = 1 + \sum_{n=1}^{\infty}0 = 1,$$

(recall that $0^0 = 0$, or if you don't like that, simply use the expansion of $B(0)$), we see that

$$ce^{e^0} = ce^1 = ce = 1,$$

so $c = e^{-1}$. Hence

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

There are techniques to extract coefficients from expressions like this, also, but we will not cover these techniques in this class.

EXERCISES 9.11.

1) Find B_4.

2) What is the exponential generating function for the sequence $a_i = i!$ for every $i \geq 0$? Give the sequence in both an expanded and a closed form.

3) What is the exponential generating function for the sequence $b_i = (i+1)!/2$ for every $i \geq 0$? Give the sequence in both an expanded and a closed form.

SUMMARY:

- generating functions must start with a 0th term
- Important definitions:
  - ○ derangements
  - ○ Catalan numbers
  - ○ exponential generating function
  - ○ Bell numbers

Chapter 10

Other Basic Counting Techniques

There are two other elementary techniques that are surprisingly useful even in quite difficult counting problems. We will wrap up our exploration of enumeration by discussing these techniques.

10A. The Pigeonhole Principle

The Pigeonhole Principle is a technique that you can apply when you are faced with items chosen from a number of different categories of items, and you want to know whether or not some of them must come from the same category, without looking at all of the items.

EXAMPLE 10.1. Suppose I will be teaching an independent study course in graph theory to two students next semester, and I want to use Bondy & Murty's "Graph Theory" text book. It has been issued in two editions, and I don't care which edition we use, but I want both students to have the same edition.

I find a web site on which someone has posted that they have three copies of the text for sale, but they don't say which editions they are. Without any more information, I know that if I buy these texts, I will have suitable texts for my students.

The reasoning is straightforward. The first book could be edition 1 or edition 2. If the second text is the same as the first, then I have what I need, so the only possible problem is if the first two books consist of one copy of edition 1, and one copy of edition 2. But then the third book must match one or the other of the first two, since there are only two editions, so I will have two copies of one or the other of the editions.

This idea can be generalised in several ways. We'll look at the most straightforward generalisation first.

PROPOSITION 10.2. Pigeonhole Principle *If there are n items that fall into m different categories and $n > m$, then at least two of the items must fall into the same category.*

PROOF. Amongst the first m items, either two of the items are from the same category (so we are done), or there is exactly one item from each of the m categories. Since $n > m$, there is at least one more item. This item must fall into the same category as one of the previous items, since every category already has an item. □

The name of this principle comes from the idea that it can be stated with the categories being a row of holes, and the items being pigeons who are assigned to these holes.

In Example 10.1, the categories were the editions, and the items were the text books.

Example 10.1 was a very direct and straightforward application of the Pigeonhole Principle. The Principle can also apply in much more subtle and surprising ways.

EXAMPLE 10.3. Maria makes a bet with Juan. He must buy her at least one chocolate bar every day for the next 60 days. If, at the end of that time, she cannot point out a span of consecutive days in which the number of chocolate bars he gave her was precisely 19, then she will pay for all of the chocolate bars and give them back to him. If she can find such a span, then she gets to keep the chocolate bars. To limit the size of the bet, they agree in advance that Juan will not buy more than 100 chocolate bars in total.

Is there a way for Juan to win this bet?

SOLUTION. The answer is no. For $1 \leq i \leq 60$, let a_i represent the number of chocolate bars that Juan has bought for Maria by the end of day i. Then $1 \leq a_1 < a_2 < \ldots < a_{60} \leq 100$. Maria is hoping that for some $i < j$, she will be able to find that $a_i + 19 = a_j$. We therefore also need to consider the values $a_1 + 19 < a_2 + 19 < \ldots < a_{60} + 19$. By the bounds on a_1 and a_{60}, we have $a_1 + 19 \geq 20$, and $a_{60} + 19 \leq 119$. Thus, the values $a_1, \ldots, a_{60}, a_1 + 19, \ldots, a_{60} + 19$ are 120 numbers all of which lie between 1 and 119.

By the Pigeonhole Principle, at least two of these numbers must be equal, but we know that the a_is are strictly increasing (as are the $a_i + 19$s), so there must exist some $i < j$ such that $a_i + 19 = a_j$. Maria must point to the span of days from the start of day $i + 1$ to the end of day j, since in this span Juan gave her 19 chocolate bars.

In fact, Juan could not win a bet of this nature that lasted more than 56 days, but proving this requires more detailed analysis specific to the numbers involved, and is not really relevant to this course. □

Here is another example that would be hard to prove if you didn't know the Pigeonhole Principle.

EXAMPLE 10.4. Fix n, and colour each point of the plane with one of n colours. Prove that there exists a rectangle whose four corners are the same colour.

SOLUTION. Proof. Take a grid of points with $n + 1$ rows and $n\binom{n+1}{2} + 1$ columns. We claim that this grid will contain such a rectangle.

Since n colours have been used, and there are $n+1$ points in each column, by the Pigeonhole Principle each column must contain at least two grid points that are the same colour.

In any column, there are $\binom{n+1}{2}$ possible locations in which a pair of points of the same colour could appear. Thus there are at most $\binom{n+1}{2}$ ways to position two points of colour 1 in a column so that the points do not occupy the same two locations in more than one of these columns. The same is true for each of the n colours. Therefore, we can create a maximum of $n\binom{n+1}{2}$ columns, each having two points of some colour, in such a way as to avoid having the same colour occupy the same two locations in more than one of the columns. Since we have $n\binom{n+1}{2} + 1$ columns, there must exist some pair of columns such that the same colour does occupy the same two locations in both of the columns. These four points form a rectangle whose corners all have the same colour. □

So far we have only thought about guaranteeing that there are at least two items in some category. Sometimes we might want to know that there are at least k items in some category, where $k > 2$. There is a generalisation of the Pigeonhole Principle that applies to such situations.

PROPOSITION 10.5. Generalised Pigeonhole Principle *Given n items that fall into m different categories, if $n > km$ for some positive integer k, then at least $k+1$ of the items must fall into the same category.*

PROOF. Amongst the first km items, either $k+1$ of the items are from the same category (so we are done), or there are exactly k items from each of the m categories. Since $n > km$, there is at least one more item. This item must fall into the same category as one of the previous items. Since every category already has k items, this means that there will be $k+1$ items in this category. □

Notice that the Pigeonhole Principle is a special case of the Generalised Pigeonhole Principle, obtained by taking $k = 1$.

EXAMPLE 10.6. The population of West Lethbridge in the 2014 census was $35,377$.

Show that at least 97 residents of West Lethbridge share a birthday. If you live in West Lethbridge, how many people can you be sure have the same birthday as you?

SOLUTION. For the first part of this question, we apply the generalised pigeonhole principle, with $m = 366$ (for the 366 days of the year, counting February 29 since it is just as legitimate a birthday as any other despite being more uncommon), $k = 96$, and $n = 35,377$. We have

$$n = 35,377 > km = 96 \cdot 366 = 35,136,$$

so the Generalised Pigeonhole Principle tells us that at least $k+1 = 97$ people must share a birthday.

For the second part of the question, the answer is 0. There is no reason why every single other person in West Lethbridge might not have their birthday on the day after yours (although that particular possibility is quite unlikely). There is certainly no guarantee that any of them has the same birthday as yours. □

Notice that although we have found in the above example that some group of at least 97 people in West Lethbridge must have the same birthday, we have no idea of which 97 people are involved, or of what the joint birthday is. This is rather remarkable, but is an example of a type of proof that is quite common in advanced mathematics. Such proofs are referred to as "non-constructive," since they prove that something exists, without giving you any idea of how to find (or construct) such a thing.

The proof of following theorem involves a more subtle application of the Generalised Pigeonhole Principle.

THEOREM 10.7. Erdös-Szekeres Theorem *For every pair of integers $a, b \geq 1$, if S is a sequence of $ab+1$ distinct real numbers, then there is either an increasing subsequence of length $a+1$ or a decreasing subsequence of length $b+1$ in S.*

PROOF. Define a function f that maps each element of S to the length of the longest increasing subsequence that begins with that element.

If there exists some $s \in S$ such that $f(s) \geq a+1$, then we are done. So we may assume that $f(s) \leq a$ for every $s \in S$. Since there is always an increasing sequence of length at least 1 starting at any element of S, we in fact have $1 \leq f(s) \leq a$ for every $s \in S$, so there are a possible values for the outputs of f. Since $|S| = ab+1$, and $ab+1 > ab$, the Generalised Pigeonhole Principle tells us that at least $b+1$ elements of S must have the same output under the function f.

We claim that if x is before y in S and $f(x) = f(y)$, then $x > y$. By assumption, $x \neq y$ (all values of S are distinct), so the only other possibility is $x < y$. If $x < y$, then taking x followed by an increasing subsequence of length $f(y)$ that starts at y, would give an increasing subsequence of length $f(y)+1$ that starts at x, contradicting $f(x) = f(y)$. This contradiction shows that $x < y$ is not possible, so $x > y$, as claimed.

Let $s_1, s_2, \ldots, s_{b+1}$ be elements of S that have the same output under f, and appear in this order. Then by the claim we proved in the previous paragraph, $s_1 > s_2 > \ldots > s_{n+1}$, which is a decreasing subsequence of length $b+1$. □

In fact, $ab+1$ is the smallest possible length for S that guarantees this property. For any a, b, there is a sequence of length ab in which the longest increasing sequence has length a and the longest decreasing subsequence has length b. One such sequence is

$$b, b-1, \ldots, 1; 2b, 2b-1, \ldots, b+1; \ldots; ab, ab-1, \ldots, (a-1)b+1.$$

Any increasing subsequence can only have one entry from each of the a subsequences of length b that are separated by semicolons, so can only have length a. Any decreasing subsequence must be entirely contained within one of the subsequences of length b that are separated by semicolons, so can only have length b.

PROPOSITION 10.8. Even more generalised pigeonhole principle *Let $n_1, n_2, \ldots, n_m$ be positive integers. Given at least*

$$n_1 + n_2 + \ldots + n_m - m + 1$$

items that fall into m categories, there must be some $1 \le i \le m$ such that at least n_i items fall into the ith category.

PROOF. Amongst the first

$$n_1 + n_2 + \ldots + n_m - m$$

items, either there is some $1 \le i \le m$ such that at least n_i of the items fall into the ith category, or there are precisely $n_i - 1$ objects in the ith category, for every $1 \le i \le m$. Since there is at least one more item, this item must fall into the ith category for some $1 \le i \le m$, which means that there will be n_i items in this category. □

Notice that the Generalised Pigeonhole Principle is a special case of the "Even more generalised pigeonhole principle," obtained by taking

$$n_1 = n_2 = \ldots = n_m = k.$$

EXAMPLE 10.9. Suppose Ali owes Tomas \$10, and wants to give him a number of identical pieces of currency to pay her debt. Her bank only gives out currency in loonies, twonies, five-dollar bills, or ten-dollar bills, and does not take requests for specific kinds of currency. How much money must Ali request from the teller, if she wants to be sure to have \$10 in identical pieces of currency with which to pay Tomas?

SOLUTION. If Ali gets any \$10 bills she can give one of those to Tomas and is done. If she gets at least two \$5 bills, she is done. If she gets at least five twonies, she is done, and if she gets at least 10 loonies she is done. So the most money she can get without being able to give Tomas his \$10 in a single type of currency, is 9 loonies, 4 twonies, and a \$5 bill, for a total of \$22. Therefore, if Ali asks for \$23, she is guaranteed to be able to pay Tomas in a single type of currency. □

Although the above example does not directly use the "Even more generalised pigeonhole principle" because it asks for the value of the currency Ali needs to request rather than the number of items she must request, it uses the same ideas and should be helpful in understanding the concept.

EXERCISES 10.10.

1) Show that in any positioning of 17 rooks on an 8-by-8 chessboard, there must be at least three rooks none of which threaten each other (i.e. no two of which lie in the same row or column).
2) Sixteen people must sit in a row of eighteen chairs. Prove that somewhere in the row there must be six adjacent chairs all occupied.
3) An artist has produced a large work of art to be carried in a parade. Part of the concept is that it must be carried by people of roughly the same size (i.e., either all adults, or all children). The artist has left it to the last minute to find people to carry this, and is in a bit of a panic. He doesn't know if he will be able to assemble enough of either adults or children to carry the piece, so he decides to ask everyone he sees, until he has enough volunteers. It takes 15 adults to carry the piece, or 23 children. If everyone approached agrees to help, how many people does the artist need to approach before he is sure to have enough people to carry his art in the parade?
4) Let n be odd, let a be even, and let $\pi : \{1,\ldots,n\} \to \{1,\ldots,n\}$ be a permutation. Prove that the product

$$(a+1-\pi(1))(a+2-\pi(2))\cdots(a+n-\pi(n))$$

is even. Is the same conclusion necessarily true if n is even or if a is odd? Give a proof or a counterexamples in each case.
5) Let $n \geq 1$, let x be a positive integer, and let S be a subset of cardinality $n+1$ from $\{x, x^2, \ldots, x^{2n}\}$. Prove that there exist two numbers in S whose product is x^{2n+1}.
6) Show that in every set of $n+1$ distinct integers, there exist two elements a and b such that $a-b$ is divisible by n.
7) A drawer contains socks of 8 different colours. How many socks must you pull out of the drawer to be certain that you have two of the same colour?
8) There are 15 students in a Combinatorics class. Explain how you know that two of them have their birthday in the same month.
9) A pizza restaurant has 8 different toppings. Every day in October, they will put a 2-topping pizza on sale. Prove that the same pizza will be on sale on two different days.
10) Suppose A is a set of 10 natural numbers between 1 and 100 (inclusive). Show that two different subsets of A have the same sum. For example, if

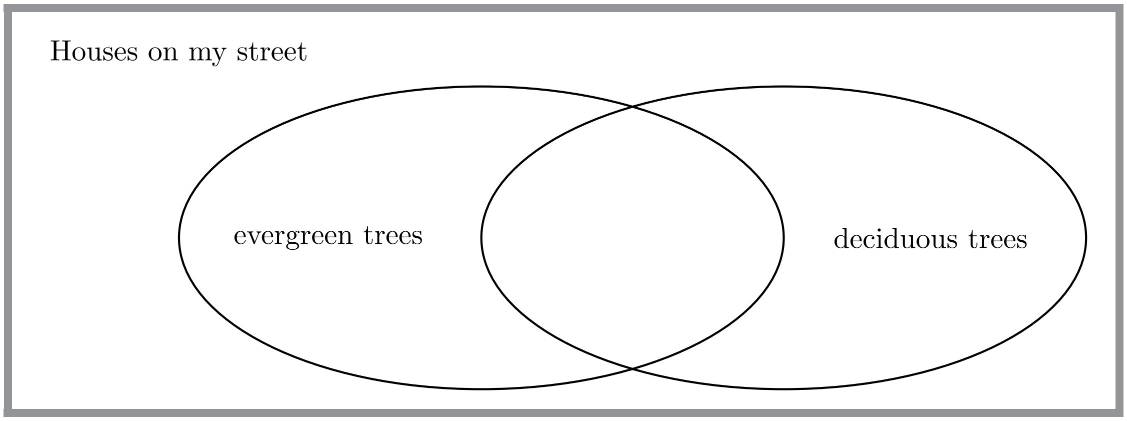
$$A = \{2, 6, 13, 30, 45, 59, 65, 82, 88, 97\},$$

then the subsets $\{6, 13, 45, 65\}$ and $\{2, 30, 97\}$ both add up to 129.

[*Hint:* Compare the answers to two questions: How many subsets of A are there? Since there are only 10 elements of A, and each of them is at most 100, how many different possible sums are there?]
11) Consider any set of 5 points in the plane that have integer coordinates. Prove that there is some pair from these 5 points such that the midpoint of the line segment joining this pair of points also has integer coordinates. Give an example of 4 points in the plane that do not have this property, and list all of the midpoints as evidence.

10B. Inclusion-Exclusion

In school, you probably saw Venn diagrams sometimes, showing groups that overlapped with one another. We could draw a very basic Venn diagram showing the kinds of trees that are growing at the various houses on my street:



Looking at the Venn diagram can help us figure out the values of some of the pieces from knowing the values of others. Suppose we know how many houses have deciduous trees, and how many houses have evergreen trees. Naïvely, you might think that adding these together would give us the total number of houses with trees. However, by looking at the Venn diagram, we see that if we simply add the values together, then any houses that have both kinds of trees have been counted twice (once as a house with a deciduous tree, and again as a house with an evergreen tree). So in order to work out the number of houses that have trees, we can add the number that have deciduous trees to the number that have evergreen trees *and then subtract the number that have both kinds of trees.* This is the idea of "inclusion-exclusion."

Specifically, if two sets A and B are disjoint, then $|A \cup B| = |A| + |B|$. However, if A and B are not disjoint, then $|A| + |B|$ counts the elements of $A \cap B$ twice (both as elements of A and as elements of B). Subtracting this overcount yields the correct answer:

PROPOSITION 10.11 (Inclusion-Exclusion for 2 sets)**.** *For any finite sets A and B, we have*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

PROOF. Let $A_0 = A \smallsetminus B$ and $B_0 = B \smallsetminus A$, so

- A is the disjoint union of A_0 and $A \cap B$,
- B is the disjoint union of B_0 and $A \cap B$, and
- $A \cup B = \big(A_0 \cup (A \cap B)\big) \cup \big(B_0 \cup (A \cap B)\big)$ is the disjoint union of A_0, B_0, and $A \cap B$.

Then

$$\begin{aligned} |A| + |B| &= \big(|A_0| + |A \cap B|\big) + \big(|B_0| + |A \cap B|\big) \\ &= \big(|A_0| + |B_0| + |A \cap B|\big) + |A \cap B| \\ &= |A \cup B| + |A \cap B|. \end{aligned}$$

□

EXAMPLE 10.12. Let $A = \{\mathsf{p}, \mathsf{r}, \mathsf{o}, \mathsf{n}, \mathsf{g}\}$ and $B = \{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$. Then

$$|A| = 5,\ |B| = 5, \text{ and } |A \cap B| = |\{\mathsf{r}, \mathsf{o}, \mathsf{n}\}| = 3,$$

so Inclusion-Exclusion tells us that

$$|A \cup B| = |A| + |B| - |A \cap B| = 5 + 5 - 3 = 7.$$

This is correct, since

$$|A \cup B| = |\{\mathsf{p}, \mathsf{r}, \mathsf{o}, \mathsf{n}, \mathsf{g}, \mathsf{h}, \mathsf{s}\}| = 7.$$

EXAMPLE 10.13. Every one of the 4000 students at Modern U owns either a tablet or a smart watch (or both). Surveys show that:

- 3500 students own a tablet, and
- 1000 students own a smart watch.

How many students own *both* a tablet and a smart watch?

SOLUTION. Let

- S be the set of all students at Modern U,
- T be the set of students who own a tablet, and
- W be the set of students who own a smart watch.

Then, by assumption,

$$|S| = 4000, \qquad |T| = 3500, \qquad |W| = 1000.$$

Since every student owns either a tablet or a smart watch, we have $S = T \cup W$. Therefore, Inclusion-Exclusion tells us that

$$|S| = |T \cup W| = |T| + |W| - |T \cap W|,$$

so

$$|T \cap W| = |T| + |W| - |S| = 3500 + 1000 - 4000 = 500.$$

Hence, there are exactly 500 students who own both a tablet and a smart watch. □

The following exercise provides a formula for the union of three sets A, B, and C. The idea is that $A \cap B$, $A \cap C$ and $B \cap C$ have all been overcounted. However, subtracting all of these will overcompensate, because the elements of $A \cap B \cap C$ have been subtracted too many times, so they need to be added back in.

EXERCISE 10.14. Suppose A, B, and C are finite sets. Show

$$\begin{aligned}|A \cup B \cup C| = |A| + |B| + |C|& \\ - |A \cap B| - |A \cap C| - |B \cap C|& \\ + |A \cap B \cap C|.&\end{aligned}$$

[*Hint:* We have formulas for $|(A \cup B) \cup C|$ and $|A \cup B|$. The equality $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ provides another useful formula.]

The following general formula calculates the cardinality of the union of any number of sets, by adding or subtracting the cardinality of every possible intersection of the sets. It is called the **Inclusion-Exclusion** formula, because it works by adding (or "including") the cardinalities of certain sets, and subtracting (or "excluding") the cardinalities of certain other sets.

THEOREM 10.15. Inclusion-Exclusion *Let $A_1, \ldots, A_n$ be finite sets. Then*

$$|A_1 \cup \ldots \cup A_n| = \left(\sum_{i=1}^{n} |A_i| \right) - \left(\sum_{1 \le i < j \le n} |A_i \cap A_j| \right) + \ldots + \left((-1)^{n+1} |A_1 \cap \ldots \cap A_n| \right).$$

Of course, we can figure out the value of any one of the terms in the inclusion-exclusion formula, if we know the values of all of the other terms.

EXAMPLE 10.16. Sandy's class is at Calaway Park. There are 21 students in the class. At the end of the day, the teacher asks some questions and determines the following:

- every student rode at least one of the roller coaster, the train, the log ride, or the bumper cars;
- 13 students rode the roller coaster;
- 6 students rode the train;
- 12 students rode the log ride;
- 15 students rode the bumper cars;
- 2 students rode all four of the rides; and
- 10 students rode at least 3 of these 4 rides.

How many students rode exactly two of the four rides?

SOLUTION. We begin by establishing some notation. Let A_1 be the set of students who rode the roller coaster; A_2 will be the set of students who rode the train; A_3 will be the set of students who rode the log ride; and A_4 will be the set of students who rode the bumper cars.

Ignoring the last piece of information for a moment, the rest of we have been given tells us that:

- $|A_1 \cup A_2 \cup A_3 \cup A_4| = 21$;
- $|A_1| = 13$;
- $|A_2| = 6$;
- $|A_3| = 12$;
- $|A_4| = 15$; and
- $|A_1 \cap A_2 \cap A_3 \cap A_4| = 2$.

The last piece of information is a bit more tricky to encode. Observe that if we take $|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|$, using ideas similar to inclusion-exclusion (or drawing the Venn diagram) we see that we have found the number of students who rode at least 3 of the 4 rides, except that we have counted the number of students who rode all 4 rides in each of the four summands, instead of counting it only once. So we need to subtract $|A_1 \cap A_2 \cap A_3 \cap A_4|$ off three times to get the number of students who rode at least 3 of the 4 rides. Since we know that $|A_1 \cap A_2 \cap A_3 \cap A_4| = 2$, this tells us that

$$|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - 6 = 10,$$

so

$$|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| = 16.$$

Thus, the inclusion-exclusion formula tells us that

$$21 = (13 + 6 + 12 + 15) - \sum_{1 \le i < j \le 4} |A_i \cap A_j| + 16 - 2,$$

so $\sum_{1 \le i < j \le 4} |A_i \cap A_j| = 39$. Unfortunately, this still isn't quite what we're looking for. The value we want is the number of students who rode exactly two of the four rides. Again, similar reasoning shows that the number of students who rode the roller coaster and the train but neither of the other two rides, will be given by:

$$|A_1 \cap A_2| - |A_1 \cap A_2 \cap A_3| - |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_2 \cap A_3 \cap A_4|.$$

Similar formulas can be worked out for each of the other five pairs that can be formed from the four rides. What we have been asked for, is the sum of these six formulas. This works out to

$$\sum_{1\leq i<j\leq 4}|A_i\cap A_j|-3\left(\sum_{1\leq i<j<k\leq 4}|A_i\cap A_j\cap A_k|\right)+6|A_1\cap A_2\cap A_3\cap A_4|=39-3(16)+6(2)=3.$$

Only three of the students rode exactly two of the four rides. □

This was a very complicated example. You should not expect to have to work out examples that are quite so tricky, but this gives you an idea of the power of inclusion-exclusion. Here is a more straightforward application.

EXAMPLE 10.17. In the Faculty of Arts and Science, the voting method used is "approval;" that is, regardless of the number of positions available, each voter can mark as many boxes as they wish on their ballot.

Imagine that Prof. Li, Prof. Cheng, and Prof. Osborn were all nominated for two computer science positions on the department's search committee. Barb Hodgson notes the following facts when counting the ballots:

- Prof. Cheng received 18 votes; Prof. Osborn received 15 votes, and Prof. Li received 10 votes.
- Only one ballot had all three boxes marked.
- Five of the ballots were marked for both Prof. Osborn and Prof. Li.
- Ten of the ballots were marked for Prof. Cheng and Prof. Osborn.
- Six of the ballots were marked for Prof. Cheng and Prof. Li.

How many members of the department voted in the election?

SOLUTION. Again, we begin by establishing some notation. Let C be the set of ballots that were marked for Prof. Cheng; let O be the set of ballots that were marked for Prof. Osborn; and let L be the set of ballots that were marked for Prof. Li. Then what we want is $|C\cup O\cup L|$: the number of ballots that were marked for at least one of the three candidates; this is the same as the number of people who voted.

Inclusion-Exclusion tells us that

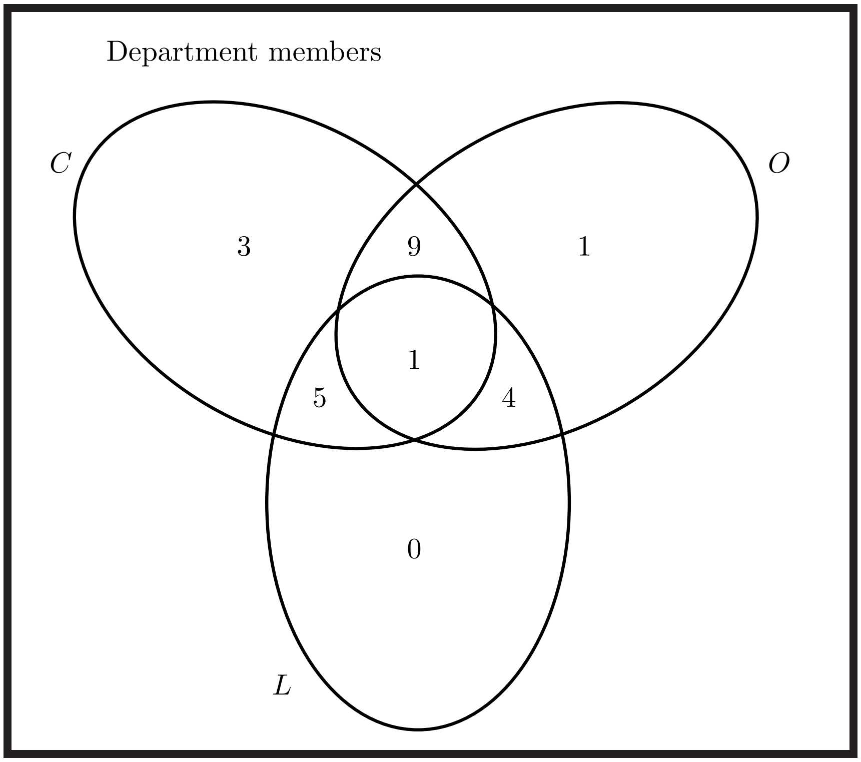
$$|C\cup O\cup L|=|C|+|O|+|L|-|C\cap O|-|C\cap L|-|O\cap L|+|C\cap O\cap L|.$$

We have been given all of the values on the right-hand side of this equation, so we see that

$$|C\cup O\cup L|=18+15+10-10-6-5+1=23.$$

There were 23 department members who voted in the election.

In fact, the information we have been given is enough for us to fill in the values in every piece of the Venn diagram.



The 9 people who voted for Prof. Cheng and Prof. Osborn but not Prof. Li is determined from the fact that 10 people voted for Professors Cheng and Osborn, and only one of those voted for all three professors. Similarly, the 4 people who voted for Prof. Li and Prof. Osborn but not Prof. Cheng is determined from the fact that 5 people voted for Professors Li and Osborn, and only one of those voted for all three professors; also, the 5 people who voted for Prof. Cheng and Prof. Li but not Prof. Osborn is determined from the fact that 6 people voted for Professors Cheng and Li, and only one of those voted for all three professors.

From the above deductions, we see that of the 18 votes Prof. Cheng received, one ballot was marked for all 3 candidates; 9 were marked for Professors Cheng and Osborn (but not Li); and 5 were marked for Professors Cheng and Li (but not Osborn). The remaining 3 votes must have been for Prof. Cheng alone, allowing us to fill in that spot. Similarly, of the 15 votes Prof. Osborn received, one ballot was marked for all 3 candidates; 9 were marked for Professors Cheng and Osborn (but not Li); and 4 were marked for Professors Osborn and Li (but not Cheng). The remaining vote must have been for Prof. Osborn alone, allowing us to fill in that spot. Finally, all of Prof. Li's 10 votes are accounted for between the 5 who voted for Professors Cheng and Li (but not Osborn), the 4 who voted for Professors Li and Osborn (but not Cheng) and the one who voted for all three, so we put a 0 into the final spot. □

EXERCISES 10.18.

1) Of 15 students in a stats class, 8 are math majors, 6 are CS majors, and 7 are in education. None are in all three, and none have any other majors. There are two math/CS joint majors, and 3 CS majors who are in education. How many math majors are in education? How many of the math majors are not in either CS or education?

2) Kevin has 165 apps on his phone. Every one of these that is not a game and was not free, requires internet access. Of these, 78 were free. Internet access is necessary for 124 of the apps to function fully. Of the apps on his phone, 101 are games. Kevin has 62 games on his phone that require internet access; 48 of these were free. Out of all

of the games on his phone, 58 were free. How many of the free apps on Kevin's phone that aren't games, require internet access?

3) How many integers between 1 and 60 are divisible by at least one of 2, 3, and 5?

4) In the 403 area code, how many of the 10-digit possible phone numbers (where any combination of digits is allowed) contain at least one of each odd digit?

5) Assume $|U| = 15$, $|V| = 12$, and $|U \cap V| = 4$. Find $|U \cup V|$.

6) Assume $|R| = 13$, $|S| = 17$, and $|R \cup S| = 25$. Find $|R \cap S|$.

7) Assume $|J| = 300$, $|J \cup L| = 500$, and $|J \cap L| = 150$. Find $|L|$.

8) At a small university, there are 90 students that are taking either Calculus *or* Linear Algebra (or both). If the Calculus class has 70 students, and the Linear Algebra class has 35 students, then how many students are taking both Calculus *and* Linear Algebra?

9) How many numbers from 1 to 5000 are divisible by either 3 or 17?

10) How many 12-digit numbers (in which the first digit is *not* 0) have either no 0 or no 5?

SUMMARY:

- Pigeonhole Principle
- Generalised Pigeonhole Principle
- Even more generalised pigeonhole principle
- Inclusion-Exclusion

Part II

Graph Theory

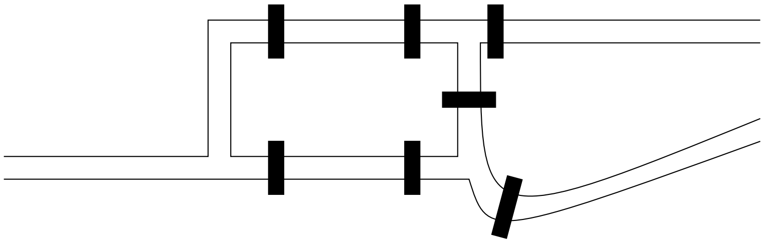
Chapter 11

Basics of Graph Theory

11A. Background

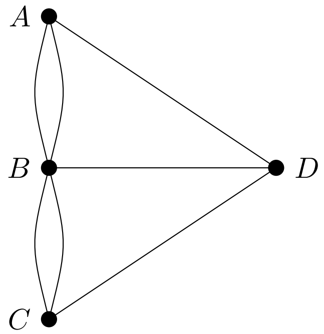
In combinatorics, what we call a *graph* has nothing to do with the x and y axes, and plotting. Here, a graph is the most straightforward way you could think of to model a network. A network could be a computer network, a road network, a telephone network; it doesn't matter what kind of network it is. Conceptually, any network consists of a bunch of things (let's call them nodes) that are being connected in some fashion. To model this, we draw some points for the nodes, and we draw edges between nodes that have a direct connection.

Leonhard Euler laid the foundations of graph theory in 1735, with his solution to the Königsberg bridge problem. Königsberg, Prussia (now Kaliningrad, Russia) was a city on the river Pregel. The city included two islands in the river, as well as land on both sides of the river, and there were seven bridges connecting the various parts of the city. The lay-out of the city and its bridges looked something like this:



The question had been posed: is it possible for residents of Königsberg, out for Sunday strolls, to cross each of the seven bridges exactly once? Better yet, can they do this *and* end up in the same part of the city where they started?

Euler modeled the problem using a graph, with a vertex for each part of the city (one for each bank, and one for each island), and edges representing the bridges. His model looked like this:



The nodes A and C represent the two banks of the river, while B and D represent the islands. In the model, the question becomes can we trace all of the edges of this graph, without lifting our pen from the paper or going over an edge more than once?

Euler was actually able to find an easy method you can use on any graph, to quickly work out whether or not this can be done for that graph. Also, unlike what we saw in the Pigeonhole Principle, his method is *constructive*: if it can be done, his method shows you how to do it. We'll go over this method later, in Chapter 13.

11B. Basic definitions, terminology, and notation

Now that we have an intuitive understanding of what a graph is, it is time to make a formal definition.

DEFINITION 11.1. A **graph** G consists of two sets:

- V, whose elements are referred to as the **vertices** of G (the singular of vertices is **vertex**); and
- E, whose elements are unordered pairs from V (i.e., $E \subseteq \{\{v_1, v_2\} \mid v_1, v_2 \in V\}$). The elements of E are referred to as the **edges** of G.

For clarity in situations where more than one graph is being studied, we may use $E(G)$ for E and $V(G)$ for V.

According to this definition, Euler's model of the bridges of Königsberg is not actually a graph, because some of the vertices have more than one edge between them (for example, there are two edges between A and B), which makes E a multiset rather than a set. This leads naturally to another definition.

DEFINITION 11.2. For some purposes, we may allow E to be a multiset rather than a set. When we do this, an element that appears more than once in E is called a **multiple edge** or **multiedge**. A graph that includes at least one multiple edge is called a **multigraph**.

Another situation that we might like to allow for some purposes but not allow for others, is the possibility of a connection that goes from a node back to itself.

DEFINITION 11.3. An edge of the form $\{v, v\}$ for some $v \in V$, is called a **loop**.

A **simple graph** is a graph that has no loops or multiple edges.

Figure 11.1. A loop.

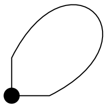
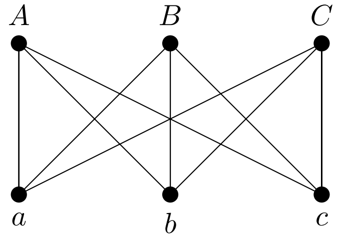


Figure 11.2. A simple graph.



For most of the graph theory we cover in this course, we will only consider simple graphs. However, there are some results for which the proof is identical whether or not the graph is simple, and other results that actually become easier to prove if we allow multigraphs and/or loops, than if we only allow simple graphs. It is worthwhile and sometimes important to think about which of our results apply to multigraphs (and/or graphs with loops), and which do not. From this point on, unless otherwise specified, you should assume that *any time the word "graph" is used, it means a simple graph.* However, be aware that many of our definitions and results generalise to multigraphs and to graphs or multigraphs with loops, even where we don't specify this.

There is still more basic terminology that we need to establish before we can say much about a graph.

DEFINITION 11.4. If $e = \{u, v\}$ is an edge of a graph (or a multigraph, with or without loops), then we say that u and v are **endvertices** (singular: endvertex) of e. We say that e is **incident with** u and v (or vice versa, the vertices are also incident with the edge), and that u and v are **adjacent** since there is an edge joining them, or that u is a **neighbour** of v.

NOTATION 11.5. We use the notation $u \sim v$ to denote that u is adjacent to v. We may also denote the edge $e = \{u, v\}$ by uv or by vu.

After one more definition, we will go through some examples using the terminology we have established.

DEFINITION 11.6. If $v \in V$ is a vertex of a graph (simple or multi, with or without loops), then the number of times v appears as the endvertex of some edge is called the **valency** of v in G. (Many sources use **degree** rather than valency, but the word degree has many meanings in mathematics, making valency a preferable term for this.) A vertex of valency 0 is called a **isolated vertex**.

Remark 11.7. In a graph without loops, we can define the valency of any vertex v as the number of edges incident with v. For most purposes, this is a good way to think of the valency. However, when a graph has loops, many formulas work out more nicely if we consider each loop to contribute 2 to the valency of its endvertex. This fits the definition we have given, since a vertex v appears twice as the endvertex of any loop incident with v.

NOTATION 11.8. The valency of v is denoted by $\text{val}(v)$ or $\deg(v)$ or $d(v)$ or $d_G(v)$.

EXAMPLE 11.9. In Figure 11.2, the vertices are a, b, c, A, B, and C, and

$$E = \{\{a, A\}, \{a, B\}, \{a, C\}, \{b, A\}, \{b, B\}, \{b, C\}, \{c, A\}, \{c, B\}, \{c, C\}\}.$$

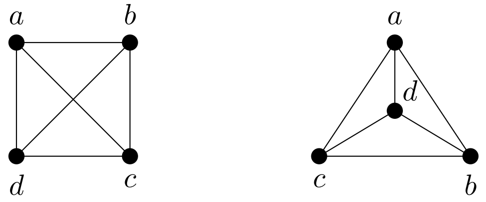
Perhaps you can see already why most people prefer to use a diagram rather than a list of vertices and edges to describe a graph!

The vertex a is adjacent to A, B and C. The vertex C is not adjacent to B. The edge $\{a, C\}$ is incident with the vertex a; the vertex C is also an endvertex of this edge. Every vertex in this graph has valency 3, so none of the vertices is isolated. This is a simple graph, as it has no loops or multiple edges.

Although a diagram is a convenient and often helpful way to visualise a graph, it is important to note that because a graph is defined by the sets V and E, it is often possible to draw a particular graph in ways that look quite different. Despite the different-looking drawings, as long as V and E are the same, the graph is also the same. In Figure 11.3, we see two different drawings of the graph given by $V = \{a, b, c, d\}$ and

$$E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}.$$

Figure 11.3. Two different drawings of the same graph.



EXAMPLE 11.10. Let the graph G be defined by $V = \{w, x, y, z\}$ and $E = \{e_1, e_2\}$, where $e_1 = \{w, x\}$ and $e_2 = \{w, y\}$. There are no loops or multiple edges, so G is a simple graph. The edge e_2 has endvertices w and y. The vertex w is incident with both e_1 and e_2. The vertices x and y are not adjacent. The vertex z is an isolated vertex, as it has no neighbours. The vertex y has only one neighbour, w. The valency of w is 2. The valency of x and the valency of y are both 1. In verifying all of these statements, drawing a diagram of the graph might help you.

EXERCISES 11.11. For each of the following graphs (which may or may not be simple, and may or may not have loops), find the valency of each vertex. Determine whether or not the graph is simple, and if there is any isolated vertex. List the neighbours of a, and all edges with which a is incident.

1) Let G be defined by $V = \{a, b, c, d, e\}$ and $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ with $e_1 = \{a, c\}$, $e_2 = \{b, d\}$, $e_3 = \{c, d\}$, $e_4 = \{c, e\}$, $e_5 = \{d, e\}$, and $e_6 = \{e, e\}$.
2) Let G be defined by $V = \{a, b, c\}$ and $E = \{e_1, e_2, e_3\}$ with $e_1 = \{a, b\}$, $e_2 = \{a, c\}$, and $e_3 = \{a, c\}$.
3) Let G be defined by $V = \{a, b, c, d\}$ and $E = \{e_1, e_2, e_3\}$ with $e_1 = \{a, b\}$, $e_2 = \{a, c\}$, and $e_3 = \{b, c\}$.

EXERCISES 11.12.

1) Let G be the graph whose vertices are the 2-element subsets of $\{1, 2, 3, 4, 5\}$, with vertices $\{a, b\}$ and $\{c, d\}$ adjacent if and only if $\{a, b\} \cap \{c, d\} = \emptyset$. Draw G.
2) The number of edges in the k-dimensional cube Q_k (which is an important structure in network design, but you do not need to know the structure to solve this) can be found by the recurrence relation:

$$e(Q_0) = 0;\ e(Q_n) = 2e(Q_{n-1}) + 2^{n-1} \text{ for } n \geq 1.$$

Use generating functions to solve this recurrence relation and therefore determine the number of edges in the k-dimensional cube.

11C. Deletion, complete graphs, and the Handshaking Lemma

We'll begin this section by introducing a basic operation that can change a graph (or a multigraph, with or without loops) into a smaller graph: deletion.

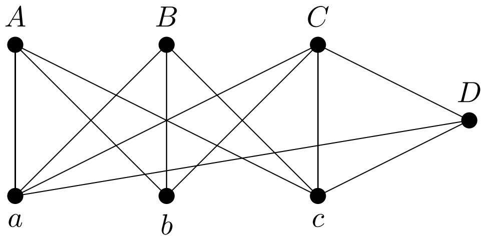
DEFINITION 11.13. Start with a graph (or multigraph, with or without loops) G with vertex set V and edge set E, and some vertex $v \in V$. If we **delete the vertex v** from the graph G, the resulting graph has vertex set $V \setminus \{v\}$ and edge set

$$E \setminus \{e \mid e \text{ is incident with } v\}.$$

NOTATION 11.14. The graph obtained by deleting the vertex v from G is denoted by $G \setminus \{v\}$. We can delete more than one vertex; for any set $S \subseteq V$ of vertices of G, we use $G \setminus S$ to denote the graph obtained by deleting all of the vertices of S from G.

The graph $G \setminus \{v\}$ might be a multigraph, but only if G is. It could have loops, but only if G has loops.

If we begin with the graph



and delete the vertex D, then we obtain the graph shown in Figure 11.2.

We can also delete edges, rather than vertices.

DEFINITION 11.15. Start with a graph (or multigraph, with or without loops) G with vertex set V and edge set E, and some edge $e \in E$. If we **delete the edge e** from the graph G, the resulting graph has vertex set V and edge set $E \setminus \{e\}$.

NOTATION 11.16. The graph obtained by deleting the edge e from G is denoted by $G \setminus \{e\}$. We can delete more than one edge; for any set $T \subseteq E$ of edges of G, we use $G \setminus T$ to denote the graph obtained by deleting all of the edges of T from G.

The graph $G \setminus \{e\}$ might be a multigraph, but only if G is. It could have loops, but only if G has loops.

Notice that deleting the edges $\{C, D\}$, $\{a, D\}$ and $\{c, D\}$ from the graph drawn above, does *not* result in the graph shown in Figure 11.2, because the graph we obtain by deleting these edges still has the vertex D (as an isolated vertex), whereas the graph shown in Figure 11.2 has only the six vertices $\{a, b, c, A, B, C\}$.

Vertex and edge deletion will be very useful for using proofs by induction on graphs (and multigraphs, with or without loops). It is handy to have terminology for a graph that can be obtained from another graph by deleting vertices and/or edges.

DEFINITION 11.17. Let G be a graph. If H can be obtained from G by deleting vertices and/or edges, then H is a **subgraph** of G. A subgraph H of G is **proper** if $H \neq G$.

We now define a very important family of graphs, called *complete graphs.*

DEFINITION 11.18. A (simple) graph in which every vertex is adjacent to every other vertex, is called a **complete graph**. If this graph has n vertices, then it is denoted by K_n.

The notation K_n for a complete graph on n vertices comes from the name of Kazimierz Kuratowski, a Polish mathematician who lived from 1896–1980. Although his main area of research was logic, Kuratowski proved an important theorem that involves a complete graph. We'll study his theorem later in the course.

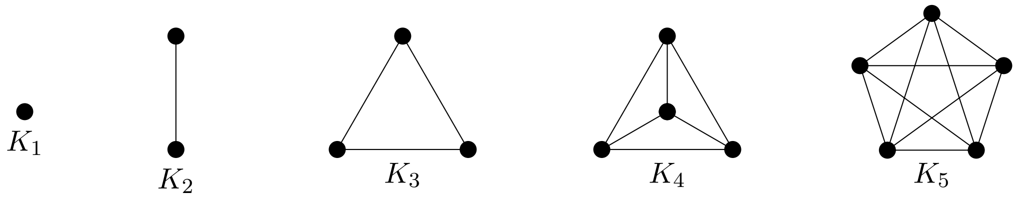
With this set-up, we are ready to prove our first result about graphs.

PROPOSITION 11.19. *The number of edges of* K_n *is* $\frac{n(n-1)}{2} = \binom{n}{2}$.

We present two proofs of this proposition: first, a combinatorial proof; then, a proof by induction.

COMBINATORIAL PROOF. A complete graph has an edge between any pair of vertices. From n vertices, there are $\binom{n}{2}$ pairs that must be connected by an edge for the graph to be complete. Thus, there are $\binom{n}{2}$ edges in K_n. □

Before giving the proof by induction, let's show a few of the small complete graphs. In particular, we'll need to have K_1 in mind as it will be the base case for our induction.



PROOF BY INDUCTION. Base case: $n = 1$. As we can see above, the graph K_1 has 0 edges. Also,

$$n(n-1)/2 = 1(0)/2 = 0.$$

So the equality holds for $n = 1$. This completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 1$ be arbitrary, and suppose that K_k has $\binom{k}{2}$ edges.

We want to deduce that K_{k+1} has $\binom{k+1}{2}$ edges. Start with K_{k+1}, and let the number of edges of this graph be t. Now we delete a vertex v from K_{k+1}. By the definition of vertex deletion, we must delete every edge incident with v. Since K_{k+1} is complete, v is adjacent to every other vertex, so there are k edges incident with v, and it is precisely these edges that we have deleted. There must be $t - k$ edges remaining.

Notice that deleting v does not affect edges that are not incident with v. Therefore, if we consider any two vertices in the remaining graph, they will still be adjacent (since they were adjacent in K_{k+1} and the edge between them was not deleted). Thus, the remaining graph is K_k.

Using our inductive hypothesis, we know that K_k has $k(k-1)/2$ edges. We have shown that $t - k = k(k-1)/2$, so

$$t = \frac{k(k-1)}{2} + k = k\left(\frac{k-1}{2} + 1\right) = \frac{k(k+1)}{2} = \binom{k+1}{2},$$

which is what we wanted to deduce. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, K_n has $\binom{n}{2}$ vertices for every $n \geq 1$. □

Although this proof by induction may seem ridiculously long and complicated in comparison with the combinatorial proof, it serves as a relatively simple illustration of how proofs by induction can work on graphs. This can be a very powerful technique for proving results about graphs.

Here is another result that can be proven using either a combinatorial proof, or a proof by induction.

LEMMA 11.20. Euler's handshaking lemma *For any graph (or multigraph, with or without loops)*

$$\sum_{v \in V} d(v) = 2|E|.$$

This is called the handshaking lemma because it is often explained using vertices to represent people, and edges as handshakes between people. In this explanation, the lemma says that if you add up all of the hands shaken by all of the people, you will get twice the number of handshakes that took place. This is an example of using two ways to count pairs $(v, e) \in V \times E$ such that v is incident with e, a notion that we discussed briefly when we introduced combinatorial proofs.

COMBINATORIAL PROOF. For the left-hand side of the equation, at every vertex we count the number of edges incident with that vertex. To get the right-hand side from this, observe that this process results in every edge having been counted exactly twice (once at each of its two endvertices; or, in the case of a loop, twice at its single endvertex since both ends are there).□

Although from the right perspective the handshaking lemma might seem obvious, it has a very important and useful corollary.

COROLLARY 11.21. *Every graph has an even number of vertices of odd valency.*

PROOF. Since the sum of all of the valencies in the graph is even (by Euler's handshaking lemma, Lemma 11.20), the number of odd summands in this sum must be even. That is, the number of vertices that have odd valency must be even. □

EXERCISES 11.22.

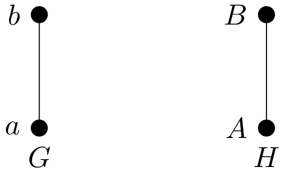
1) Give a proof by induction of Euler's handshaking lemma for simple graphs.
2) Draw K_7.
3) Show that there is a way of deleting an edge and a vertex from K_7 (in that order) so that the resulting graph is complete. Show that there is a way of deleting an edge and a vertex from K_7 (in that order) so that the resulting graph is not complete.
4) Prove Corollary 11.21 by induction on the number of edges. (Use edge deletion, and remember that the base case needs to be when there are no edges.)
5) Use graphs to give a combinatorial proof that

$$\sum_{i=1}^{k} \binom{n_i}{2} \leq \binom{n}{2},$$

where $n_1, n_2, \ldots, n_k$ are positive integers with $\sum_{i=1}^{k} n_i = n$. Under what circumstances does equality hold?

11D. Graph isomorphisms

There is a problem with the way we have defined K_n. A graph is supposed to consist of two sets, V and E. Unless the elements of the sets are labeled, we cannot distinguish amongst them. Here are two graphs, G and H:



Which of these graphs is K_2? They can't both be K_2 since they aren't the same graph – can they?

The answer lies in the concept of isomorphisms. Intuitively, graphs are isomorphic if they are identical except for the labels (on the vertices). Recall that as shown in Figure 11.3, since graphs are defined by the sets of vertices and edges rather than by the diagrams, two isomorphic graphs might be drawn so as to look quite different.

DEFINITION 11.23. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic** if there is a bijection (a one-to-one, onto map) φ from V_1 to V_2 such that

$$\{v, w\} \in E_1 \Leftrightarrow \{\varphi(v), \varphi(w)\} \in E_2.$$

In this case, we call φ an **isomorphism** from G_1 to G_2.

NOTATION 11.24. When φ is an isomorphism from G_1 to G_2, we abuse notation by writing $\varphi : G_1 \to G_2$ even though φ is actually a map on the vertex sets.

We also write $G_1 \cong G_2$ for "G_1 is isomorphic to G_2."

So a graph isomorphism is a bijection that preserves edges and non-edges. If you have seen isomorphisms of other mathematical structures in other courses, they would have been bijections that preserved some important property or properties of the structures they were mapping. For graphs, the important property is which vertices are connected to each other. If that is preserved, then the networks being represented are for all intents and purposes, the same.

Recall from Math 2000, a relation is called an **equivalence relation** if it is a relation that satisfies three properties. It must be:

- **reflexive** (every object must be related to itself);
- **symmetric** (if object A is related to object B, then object B must also be related to object A); and
- **transitive** (if object A is related to object B and object B is related to object C, then object A must be related to object C).

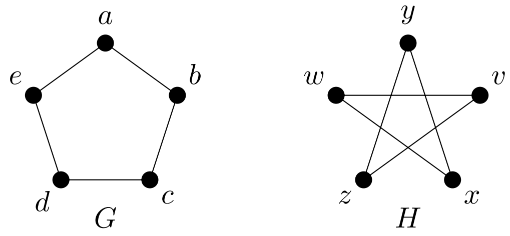
The relation "is isomorphic to" is an equivalence relation on graphs . To see this, observe that:

- for any graph G, we have $G \cong G$ by the identity map on the vertices;
- for any graphs G_1 and G_2, we have
$$G_1 \cong G_2 \Leftrightarrow G_2 \cong G_1,$$
since any bijection has an inverse function that is also a bijection, and since
$$\{v, w\} \in E_1 \Leftrightarrow \{\varphi(v), \varphi(w)\} \in E_2$$
is equivalent to
$$\{\varphi^{-1}(v), \varphi^{-1}(w)\} \in E_1 \Leftrightarrow \{v, w\} \in E_2;$$
- for any graphs G_1, G_2, and G_3 with $\varphi_1 : G_1 \to G_2$ and $\varphi_2 : G_2 \to G_3$ being isomorphisms, the composition $\varphi_2 \circ \varphi_1 : G_1 \to G_3$ is a bijection, and
$$\{v, w\} \in E_1 \Leftrightarrow \{\varphi_1(v), \varphi_1(w)\} \in E_2 \Leftrightarrow \{\varphi_2(\varphi_1(v)), \varphi_2(\varphi_1(w))\} \in E_3,$$

so $G_1 \cong G_3$.

The answer to our question about complete graphs is that any two complete graphs on n vertices are isomorphic, so even though technically the set of all complete graphs on 2 vertices is an equivalence class of the set of all graphs, we can ignore the labels and give the name K_2 to all of the graphs in this class.

EXAMPLE 11.25. The graphs G and H:



are isomorphic. The map φ defined by

- $\varphi(a) = v$;
- $\varphi(b) = z$;
- $\varphi(c) = y$;
- $\varphi(d) = x$;
- $\varphi(e) = w$

is an isomorphism. It is straightforward (though perhaps tedious) to check that each of the 5 edges of G maps to one of the five edges of H under φ.

To prove that two graphs are isomorphic, we must find a bijection that acts as an isomorphism between them. If we want to prove that two graphs are *not* isomorphic, we must show that *no* bijection can act as an isomorphism between them.

Sometimes it can be very difficult to determine whether or not two graphs are isomorphic. It is possible to create very large graphs that are very similar in many respects, yet are not isomorphic. A common approach to this problem has been attempting to find an "invariant" that will distinguish between non-isomorphic graphs. An "invariant" is a graph property that remains the same for all graphs in any isomorphism class. Thus, if you can find an invariant that is different for two graphs, you know that these graphs must not be isomorphic. We say in this case that this invariant *distinguishes between* these two graphs.

Mathematicians have come up with many, many graph invariants. Unfortunately, so far, for every known invariant it is possible to find two graphs that are not isomorphic, but for which the invariant is the same. In other words, no known invariant distinguishes between every pair of non-isomorphic graphs.

As an aside for those of you who may know what this means (probably those in computer science), the graph isomorphism is particularly interesting because it is one of a very few (possibly two, the other being integer factorisation) problems that are known to be in NP but that are not known to be either in P, or to be NP-complete.

We give a few graph invariants in the following proposition.

PROPOSITION 11.26. *If $G_1 \cong G_2$ are graphs, then*

1) G_1 and G_2 have the same number of vertices;

2) G_1 and G_2 have the same number of edges;

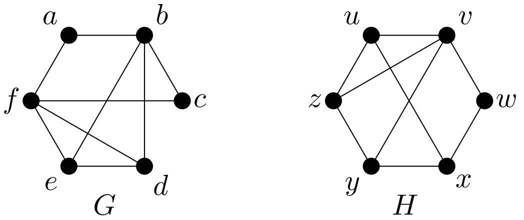
3) if we list the valency of every vertex of G_1 and do the same for G_2, the lists will be the same (though possibly in a different order). (Such a list is called the **degree sequence** *of the graph.)*

PROOF.

1) Since $G_1 \cong G_2$, there is an isomorphism $\varphi : V_1 \to V_2$ (where V_1 is the vertex set of G_1 and V_2 is the vertex set of G_2). Since φ is a bijection, we must have $|V_1| = |V_2|$.
2) Since
$$\{v, w\} \in E_1 \Rightarrow \{\varphi(v), \varphi(w)\} \in E_2,$$
we see that for every edge of E_1, there is an edge of E_2. Therefore, $|E_2| \geq |E_1|$. Similarly, since
$$\{\varphi(v), \varphi(w)\} \in E_2 \Rightarrow \{v, w\} \in E_1,$$
we see that $|E_1| \geq |E_2|$. So $|E_1| = |E_2|$.
3) If $\varphi(v_1) = v_2$ then $d_{G_1}(v_1) = d_{G_2}(v_2)$, because $u \sim v_1$ if and only if $\varphi(u) \sim v_2$. □

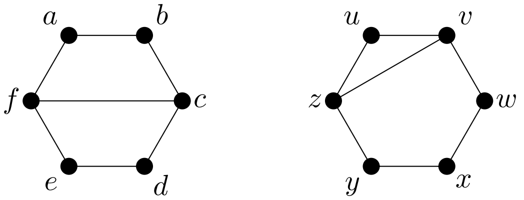
EXAMPLE 11.27. The graph G of Example 11.25 is not isomorphic to K_5, because K_5 has $\binom{5}{2} = 10$ edges by Proposition 11.19, but G has only 5 edges. Notice that the number of vertices, despite being a graph invariant, does not distinguish these two graphs.

The graphs G and H:



are not isomorphic. Each of them has 6 vertices and 9 edges. However, the graph G has two vertices of valency 2 (a and c), two vertices of valency 3 (d and e), and two vertices of valency 4 (b and f). Meanwhile, the graph H has one vertex of valency 2 (w), four vertices of valency 3 (u, x, y, and z), and one vertex of valency 4 (v). Although each of these lists has the same values (2s, 3s, and 4s), the lists are not the same since the number of entries that contain each of the values is different. In particular, the two vertices a and c both have valency 2, but there is only one vertex of H (vertex w) of valency two. Either a or c could be sent to w by an isomorphism, but either choice leaves no possible image for the other vertex of valency 2. Therefore, an isomorphism between these graphs is not possible.

Observe that the two graphs



both have 6 vertices and 7 edges, and each has four vertices of valency 2 and two vertices of valency 3. Nonetheless, these graphs are not isomorphic. Perhaps you can think of another graph invariant that is not the same for these two graphs.

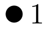
To prove that these graphs are not isomorphic, since each has two vertices of valency 3, any isomorphism would have to map $\{c, f\}$ to $\{v, z\}$. Now, whichever vertex gets mapped to u must be a mutual neighbour of c and f since u is a mutual neighbour of v and z. But c and f

have no mutual neighbours, so this is not possible. Therefore there is no isomorphism between these graphs.

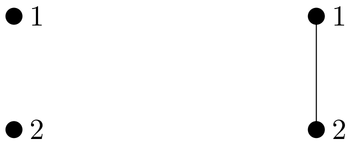
A natural problem to consider is: how many different graphs are there on n vertices? If we are not worrying about whether or not the graphs are isomorphic, we could have infinitely many graphs just by changing the labels on the vertices, and that's not very interesting. To avoid this problem, we fix the set of labels that we use. Label the vertices with the elements of $\{1, \dots, n\}$. We'll call the number of graphs we find, the number of *labeled* graphs on n vertices.

Any edge is a 2-subset of $\{1, \dots, n\}$. There are $\binom{n}{2}$ possible edges in total. Any graph is formed by taking a subset of the $n(n-1)/2$ possible edges. In Example 4.1, we learned how to count these: there are $2^{n(n-1)/2}$ subsets.

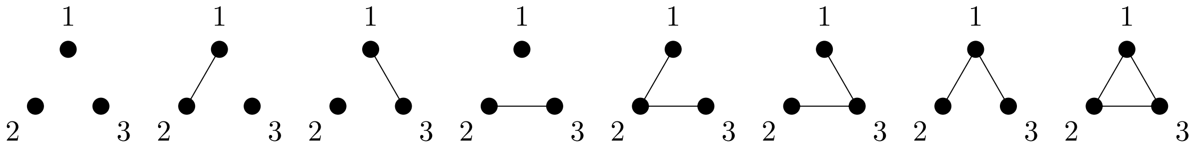
EXAMPLE 11.28. When $n = 1$, we have $\binom{1}{2} = 0$, and $2^0 = 1$, so there is exactly one labeled graph on 1 vertex. It looks like this:



When $n = 2$, we have $\binom{2}{2} = 1$, and $2^1 = 2$. so there are exactly two labeled graphs on 2 vertices. They look like this:



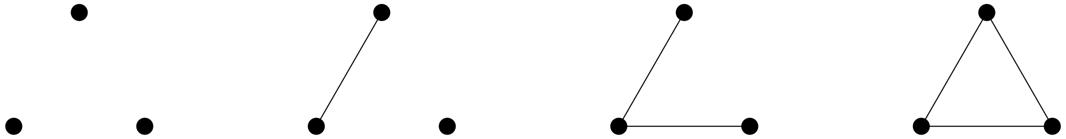
When $n = 3$, we have $\binom{3}{2} = 3$, and $2^3 = 8$, so there are exactly eight labeled graphs on 3 vertices. They look like this:



When $n = 4$, we have $\binom{4}{2} = 6$, and $2^6 = 64$, so there are exactly sixty-four labeled graphs on 4 vertices. We won't attempt to draw them all here.

Although that answer is true as far as it goes, you will no doubt observe that even though we are using a fixed set of labels, some of the graphs we've counted are isomorphic to others. A more interesting question would be, how many isomorphism classes of graphs are there on n vertices? Since we are considering isomorphism classes, the labels we choose for the vertices are largely irrelevant except to tell us which vertices are connected to which other vertices, if we don't have a diagram. Thus, if we are drawing the graphs, we usually omit vertex labels and refer to the resulting graphs (each of which represents an isomorphism class) as *unlabeled.* So the question is, how many *unlabeled* graphs are there on n vertices?

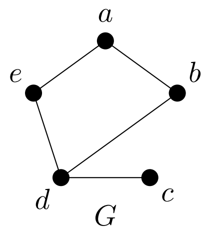
We can work out the answer to this for small values of n. From the labeled graphs on 3 vertices, you can see that there are four unlabeled graphs on 3 vertices. These are:

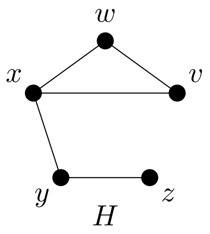


There are 11 unlabeled graphs on four vertices. Unfortunately, since there is no known polynomial-time algorithm for solving the graph isomorphism problem, determining the number of unlabeled graphs on n vertices gets very hard as n gets large, and no general formula is known.

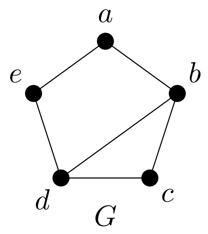
EXERCISES 11.29. For each of the following pairs of graphs, find an isomorphism or prove that the graphs are not isomorphic.

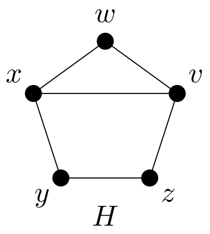
1)





2)





3) $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ with $V_1 = \{a, b, c, d\}$, $V_2 = \{A, B, C, D\}$, $E_1 = \{ab, ac, ad\}$, $E_2 = \{BC, CD, BD\}$.

EXERCISES 11.30.

1) Draw five unlabeled graphs on 5 vertices that are not isomorphic to each other.

2) How many labeled graphs on 5 vertices have 1 edge?

3) How many labeled graphs on 5 vertices have 3 or 4 edges?

SUMMARY:

- graphs are defined by sets, not by diagrams
- deleting a vertex or edge
- how to use proofs by induction on graphs
- Euler's handshaking lemma
- graph invariants, distinguishing between graphs
- labeled and unlabeled graphs
- Important definitions:
    - graph, vertex, edge
    - loop, multiple edge, multigraph, simple graph
    - endvertex, incident, adjacent, neighbour
    - degree, valency, isolated vertex
    - subgraph
    - complete graph
    - isomorphic graphs, isomorphism between graphs
- Notation:
    - $u \sim v$
    - uv
    - $\mathrm{val}(v)$, $\deg(v)$, $d(v)$, $d_G(v)$
    - $G \setminus \{v\}$, $G \setminus \{e\}$
    - K_n
    - $G_1 \cong G_2$

Chapter 12

Moving through graphs

We have some basic concepts and terminology now, but it is important to remember that graphs are models of networks. Networks are all about moving things around, whether those things are cars, data, or whatever. So if graphs are going to be useful models, routes in the network need to correspond to routes in the graph, and we need to be able to describe these routes, and to learn about them.

12A. Directed graphs

Some networks include connections that only allow travel in one direction (one-way roads; transmitters that are not receivers, etc.). These can be modeled using *directed graphs.*

DEFINITION 12.1. A **directed graph**, or **digraph** for short, consists of two sets:

- V, whose elements are the vertices of the digraph; and
- A, whose elements are ordered pairs from V, so

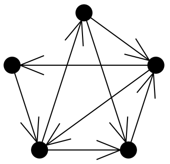
$$A \subseteq \{(v_1, v_2) \mid v_1, v_2 \in V\}.$$

The elements of A are referred to as the **arcs** of the digraph.

When drawing a digraph, we draw an arrow on each arc so that it points from the first vertex of the ordered pair to the second vertex.

Like multigraphs, we will not study digraphs in this course, but you should be aware of the basic definition. Many of the results we will cover in this course, generalise to the context of digraphs.

EXAMPLE 12.2. A digraph.



We will give one example of generalising a result on graphs, to the context of digraphs. In order to do so, we need a definition.

DEFINITION 12.3. The **outvalency** or **outdegree** of a vertex v in a digraph is the number of arcs whose first entry is v, i.e.,

$$|\{w \in V \mid (v, w) \in A\}|.$$

The **invalency** or **indegree** of a vertex v in a digraph is the number of arcs whose second entry is v.

NOTATION 12.4. The outvalency of vertex v is denoted by $d^+(v)$. The invalency of vertex v is denoted by $d^-(v)$.

LEMMA 12.5. Euler's handshaking lemma for digraphs. *For any digraph,*

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |A|.$$

COMBINATORIAL PROOF. For the left-hand side of the equation, at every vertex we count the number of arcs that begin at that vertex. Since each of these arcs ends at some vertex, we get the same result in the middle part of the equation, where at every vertex we count the number of arcs that end at that vertex. In each case, we have counted every arc precisely once, so both of these values are equal to the right-hand side of the equation, the number of arcs in the digraph. □

EXERCISES 12.6.

1) Use induction to prove Euler's handshaking lemma for digraphs that have no loops (arcs of the form (v, v) or multiarcs (more than one arc from some vertex u to some other vertex v).
2) A digraph isomorphism is a bijection on the vertices that preserves the arcs. Come up with a digraph invariant, and prove that it is an invariant.
3) List the indegree and outdegree of each vertex of the digraph from Example 12.2.

12B. Walks and connectedness

Graphs can be connected or disconnected. Intuitively, this corresponds to the network being connected or disconnected – is it possible to travel from any node to any other node? When a graph (or network) is disconnected, it has broken down into some number of separate *connected components* - the pieces that still are connected.

Since this is mathematics, we require more formal definitions, to ensure that the meanings are not open to misunderstanding. Before we can define connectedness, we need the concept of a *walk* in a graph.

DEFINITION 12.7. A **walk** in a graph G is a sequence of vertices $(u_1, u_2, \ldots, u_n)$ such that for every $1 \leq i \leq n-1$, we have $u_i \sim u_{i+1}$. (That is, consecutive vertices in the walk must be adjacent.)

A $\boldsymbol{u - v}$ **walk** in G is a walk with $u_1 = u$ and $u_n = v$. (That is, a walk that begins at u and ends at v.)

Now we can define what it means for a graph to be connected.

DEFINITION 12.8. The graph G with vertex set V is **connected** if for every $u, v \in V$, there is a $u - v$ walk.

The **connected component** of G that contains the vertex u, is

$$\{v \in V \mid \text{ there is a } u - v \text{ walk.}\}.$$

This definition of connected component seems to depend significantly on the choice of the vertex u. In fact, though, *being in the same connected component of* G is an equivalence relation on the vertices of G, so the connected components of G are a property of G itself, rather than depending on particular choices of vertices. We won't go through a formal proof that being in the same connected component is an equivalence relation (we leave this as an exercise below), but we will go through the proof of a proposition that is closely related.

PROPOSITION 12.9. *Let G be a graph, and let $u, v, w \in V(G)$. Suppose that v and w are in the connected component of G that contains the vertex u. Then w is in the connected component of G that contains the vertex v.*

PROOF. Since v and w are in the connected component of G that contains the vertex u, by definition there is a $u - v$ walk, and a $u - w$ walk. Let $(u = u_1, u_2, \dots, u_k = w)$ be a $u - w$ walk, and let $(u = v_1, v_2, \dots, v_m = v)$ be a $u - v$ walk.

We need to show that w is in the connected component of G that contains the vertex v; by definition, this is equivalent to showing that there is a $v - w$ walk. Consider the sequence of vertices:

$$(v = v_m, v_{m-1}, \dots, v_1 = u = u_1, u_2, \dots, u_k = w).$$

Since $(u = v_1, v_2, \dots, v_m = v)$ is a $u - v$ walk, consecutive vertices are adjacent, so consecutive vertices in the first part of the given sequence (from v_m through $v_1 = u$) are adjacent. Similarly, since $(u = u_1, u_2, \dots, u_k = w)$ is a $u - w$ walk, consecutive vertices are adjacent, so consecutive vertices in the last part of the given sequence (from $u = u_1$ through u_k) are adjacent. Therefore, the given sequence is in fact a $v - w$ walk, as desired. □

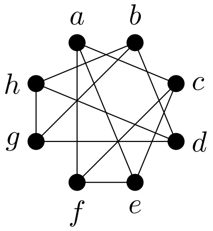
When discussing walks, it is convenient to have standard terminology for describing the length of the walk.

DEFINITION 12.10. The **length of a walk** is one less than the number of vertices in the walk. Thus, if we think of a walk as a sequence of edges (formed by consecutive pairs of vertices from the walk), the length of the walk is the number of edges in the walk.

Unfortunately, there is some disagreement amongst mathematicians as to whether the *length* of a walk should be used to mean the number of vertices in the walk, or the number of edges in the walk. We will use the latter convention throughout this course because it is consistent with the definition of the length of a cycle (which will be introduced in the next section). You should be aware, though, that you might find the other convention used in other sources.

Sometimes it is obvious that a graph is disconnected from the way it has been drawn, but sometimes it is less obvious. In the following example, you might not immediately notice whether or not the graph is connected.

EXAMPLE 12.11. Consider the following graph.



Find a walk of length 4 from a to f. Find the connected component that contains a. Is the graph connected?

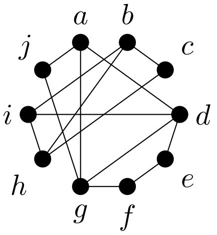
SOLUTION. A walk from of length 4 from a to f is (a, c, a, c, f). (Notice that the vertices and edges used in a walk need not be distinct.) Remember that the length of this walk is the number of edges used, which is one less than the number of vertices in the sequence!

The connected component that contains a is $\{a, c, e, f\}$. There are walks from a to each of these vertices, but there are no edges between any of these vertices and any of the vertices $\{b, d, g, h\}$.

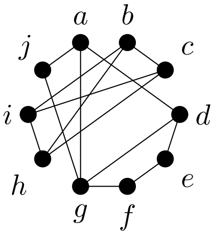
Since there is no walk from a to b (for example), the graph is not connected. □

EXERCISES 12.12.

1) Prove that *being in the same connected component of* G is an equivalence relation on the vertices of any graph G.
2) Is the following graph connected? Find the connected component that contains a. Find a walk of length 5 from a to f.



3) Is the following graph connected? Find the connected component that contains a. Find a walk of length 3 from a to d.



4) Use Euler's Handshaking Lemma to prove (by contradiction) that if G is a connected graph with n vertices and $n-1$ edges, and $n \geq 2$, then G has at least 2 vertices of valency 1.
   [*Hint:* What does G being connected imply about $d(v)$ for any vertex v of G?]
5) Fix $n \geq 1$. Prove by induction on m that for any $m \geq 0$, a graph with n vertices and m edges has at least $n - m$ connected components.

12C. Paths and cycles

Recall the definition of a walk, Definition 12.7. As we saw in Example 12.11, the vertices and edges in a walk do not need to be distinct.

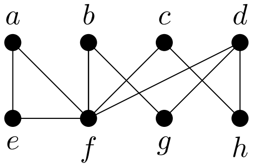
There are many circumstances under which we might not want to allow edges or vertices to be re-visited. Efficiency is one possible reason for this. We have a special name for a walk that does not allow vertices to be re-visited.

DEFINITION 12.13. A walk in which no vertex appears more than once is called a **path**.

NOTATION 12.14. For $n \geq 0$, a graph on $n+1$ vertices whose only edges are those used in a path of length n (which is a walk of length n that is also a path) is denoted by P_n. (Notice that $P_0 \cong K_1$ and $P_1 \cong K_2$.)

Notice that if an edge were to appear more than once in a walk, then both of its endvertices would also have to appear more than once, so a path does not allow vertices or edges to be re-visited.

EXAMPLE 12.15. In the graph



(a, f, c, h) is a path of length 3. However, (a, f, c, h, d, f) is not a path, even though no edges are repeated, since the vertex f appears twice. Both *are* walks.

PROPOSITION 12.16. *Suppose that u and v are in the same connected component of a graph. Then any $u-v$ walk of minimum length is a path. In particular, if there is a $u-v$ walk, then there is a $u-v$ path.*

PROOF. Since u and v are in the same connected component of a graph, there is a $u-v$ walk.

Towards a contradiction, suppose that we have a $u-v$ walk of minimum length that is not a path. By the definition of a path, this means that some vertex x appears more than once in the walk, so the walk looks like:

$$(u = u_1, \ldots, u_i = x, \ldots, u_j = x, \ldots, u_k = v),$$

and $j > i$. Observe that the following is also a $u-v$ walk:

$$(u = u_1, \ldots, u_i = x, u_{j+1}, u_{j+2}, \ldots, u_k = v).$$

Since consecutive vertices were adjacent in the first sequence, they are also adjacent in the second sequence, so the second sequence is a walk. The length of the first walk is $k-1$, and the length of the second walk is $k-1-(j-i)$. Since $j > i$, the second walk is strictly shorter than the first walk. In particular, the first walk was not a $u-v$ walk of minimum length. This contradiction serves to prove that every $u-v$ walk of minimum length is a path. □

This allows us to prove another interesting fact that will be useful later.

PROPOSITION 12.17. *Deleting an edge from a connected graph can never result in a graph that has more than two connected components.*

PROOF. Let G be a connected graph, and let uv be an arbitrary edge of G. If $G \setminus \{uv\}$ is connected, then it has only one connected component, so it satisfies our desired conclusion. Thus, we assume in the remainder of the proof that $G \setminus \{uv\}$ is not connected.

Let G_u denote the connected component of $G \setminus \{uv\}$ that contains the vertex u, and let G_v denote the connected component of $G \setminus \{uv\}$ that contains the vertex v. We aim to show that G_u and G_v are the only connected components of $G \setminus \{uv\}$.

Let x be an arbitrary vertex of G, and suppose that x is a vertex that is not in G_u. Since G is connected, there is a $u-x$ walk in G, and therefore by Proposition 12.16 there is a $u-x$ path in G. Since x is not in G_u, this $u-x$ path must use the edge $u-v$, so must start with this edge since u only occurs at the start of the path. Therefore, by removing the vertex u from the start of this path, we obtain a $v-x$ path that does not use the vertex u. This path cannot use the edge uv, so must still be a path in $G \setminus \{uv\}$. Therefore x is a vertex in G_v.

Since x was arbitrary, this shows that every vertex of G must be in one or the other of the connected components G_u and G_v, so there are at most two connected components of $G \setminus \{uv\}$. Since uv was an arbitrary edge of G and G was an arbitrary connected graph, this shows that deleting any edge of a connected graph can never result in a graph with more than two connected components. □

A cycle is like a path, except that it starts and ends at the same vertex. The structures that we will call cycles in this course, are sometimes referred to as *circuits.*

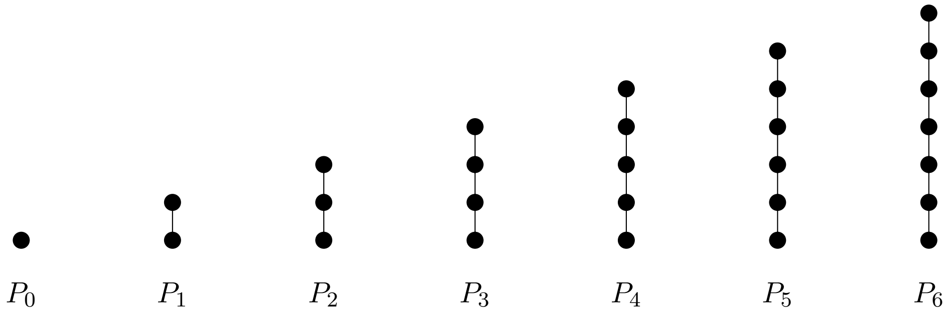
DEFINITION 12.18. A walk of length at least 1 in which no vertex appears more than once, except that the first vertex is the same as the last, is called a **cycle**.

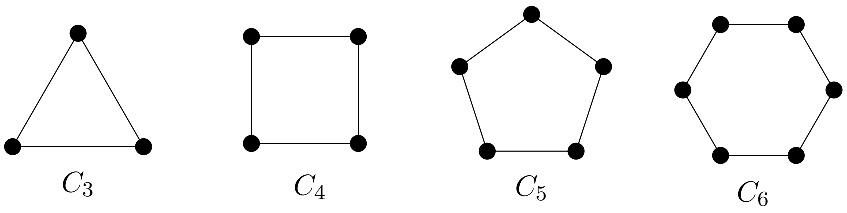
NOTATION 12.19. For $n \geq 3$, a graph on n vertices whose only edges are those used in a cycle of length n (which is a walk of length n that is also a cycle) is denoted by C_n.

The requirement that the walk have length at least 1 only serves to make it clear that a walk of just one vertex is not considered a cycle. In fact, a cycle in a simple graph must have length at least 3.

EXAMPLE 12.20. In the graph from Example 12.15, (a, e, f, a) is a cycle of length 3, and (b, g, d, h, c, f, b) is a cycle of length 6.

Here are drawings of some small paths and cycles:



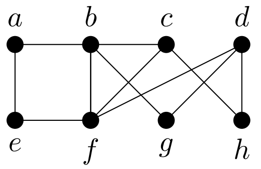


We end this section with a proposition whose proof will be left as an exercise.

PROPOSITION 12.21. *Suppose that G is a connected graph. If G has a cycle in which u and v appear as consecutive vertices (so uv is an edge of G) then $G \setminus \{uv\}$ is connected.*

EXERCISES 12.22.

1) In the graph



(a) Find a path of length 3.

(b) Find a cycle of length 3.

(c) Find a walk of length 3 that is neither a path nor a cycle. Explain why your answer is correct.

2) Prove that in a graph, any walk that starts and ends with the same vertex and has the smallest possible non-zero length, must be a cycle.

3) Prove Proposition 12.21.

4) Prove by induction that if every vertex of a connected graph on $n \geq 2$ vertices has valency 1 or 2, then the graph is isomorphic to P_n or C_n.

5) Let G be a (simple) graph on n vertices. Suppose that G has the following property: whenever $u \nsim v$, $d_G(u) + d_G(v) \geq n-1$. Prove that G is connected.

12D. Trees

A special class of graphs that arise often in graph theory, is the class of trees. If a mathematician suspects that something is true for all graphs, one of the first families of graphs for which s/he will probably try to prove it, is the family of trees, because their strong structure makes them much easier to work with than many other families of graphs.

DEFINITION 12.23. A **tree** is a connected graph that has no cycles.

A **forest** is a disjoint union of trees. So a forest is a graph that has no cycles (but need not be connected).

A **leaf** is a vertex of valency 1 (in any graph, not just in a tree or forest).

Notice that the graph P_n is a tree, for every $n \geq 1$.

We prove some important results about the structure of trees.

PROPOSITION 12.24. *Let T be a connected graph with no cycles. Then deleting any edge from T disconnects the graph.*

PROOF. If T has no edges, the statement is vacuously true. We may thus assume that T has at least one edge. Let $\{u, v\}$ be an arbitrary edge of T. (Since a loop is a cycle, we must have $u \neq v$ even if we were not assuming that our graphs are simple.)

Towards a contradiction, suppose that deleting $\{u, v\}$ from T does not disconnect T. Then by the definition of a connected graph, there is a $u - v$ walk in $T \setminus \{uv\}$. By Proposition 12.16, the shortest $u - v$ walk in $T \setminus \{uv\}$ must be a $u - v$ path. If we take this same walk in T and add u to the end, this will still be a walk in T since T contains the edge uv. Since the walk in $T \setminus \{uv\}$ was a path, no vertices were repeated. Adding u to the end of this walk makes a walk (certainly of length at least 2) in which no vertex is repeated except that the first and last vertices are the same: by definition, a cycle. Thus, T has a cycle, contradicting our hypothesis. This contradiction serves to prove that deleting any edge from T disconnects the graph. □

Since a tree is a connected graph with no cycles, this shows that deleting any edge from a tree will disconnect the graph.

PROPOSITION 12.25. *Every tree that has at least one edge, has at least two leaves.*

PROOF. We prove this by strong induction on the number of vertices. Notice that a (simple) graph on one vertex must be K_1, which has no edges, so the proposition does not apply. Therefore our base case will be when there are 2 vertices.

Base case: $n = 2$. Of the two (unlabeled) graphs on 2 vertices, only one is connected: K_2 (or P_1; these are isomorphic). Both of the vertices have valency 1, so there are two leaves. This completes the proof of the base case.

Induction step: We begin with the strong inductive hypothesis. Let $k \geq 2$ be arbitrary. Suppose that for every $2 \leq i \leq k$, every tree with i vertices has at least two leaves. (Since $i \geq 2$ and a tree is a connected graph, every tree on i vertices has at least one edge, so we may omit this part of the hypothesis.)

Let T be a tree with $k + 1$ vertices. Since $k + 1 > 1$, T has at least one edge. Choose any edge $\{u, v\}$ of T, and delete it. By Proposition 12.24, the resulting graph is disconnected. By Proposition 12.17, it cannot have more than two connected components, so it must have exactly two connected components. Furthermore, by the proof of that proposition, the components are T_u (the connected component that contains the vertex u) and T_v (the connected component that contains the vertex v).

Since T has no cycles, neither do T_u or T_v. Since they are connected components, they are certainly connected. Therefore, both T_u and T_v are trees. Since u is not a vertex of T_v and v is not a vertex of T_u, each of these trees has at most k vertices.

If both T_u and T_v have at least two vertices, then we can apply our induction hypothesis to both. This tells us that T_u and T_v each have at least two leaves. In particular, T_u must have some leaf x that is not u, and T_v must have some leaf y that is not v. Deleting uv from T did not change the valency of either x or y, so x and y must also have valency 1 in T. Therefore T has at least two leaves. This completes the induction step and therefore the proof, in the case where T_u and T_v each have at least two vertices. We must still consider the possibility that at least one of T_u and T_v has only one vertex.

Since $k + 1 \geq 3$, at least one of T_u and T_v must have two vertices, so only one of them can have only one vertex. Without loss of generality (since nothing in our argument so far made any distinction between u and v, we can switch u and v if we need to), we may assume that T_v has only one vertex, and T_u has at least two vertices. Applying our induction hypothesis to T_u, we conclude that T_u has some leaf x that is not u, and that is also a leaf of T. Furthermore, since T_v has only one vertex, this means that deleting the edge uv left v as an isolated vertex, so uv was the only edge incident with v in T. Therefore, v is a leaf of T. Thus, T has at least two leaves: x and v. This completes the induction step and therefore the proof, in the case where at least one of T_u and T_v has only one vertex. Since we have dealt with all possibilities, this completes our induction step.

By the Principle of Mathematical Induction, every tree that has at least one edge, has at least two leaves. □

The next result will be left to you to prove.

PROPOSITION 12.26. *If a leaf is deleted from a tree, the resulting graph is a tree.*

THEOREM 12.27. *The following are equivalent for a graph T with n vertices:*

1) T is a tree;

2) T is connected and has $n - 1$ edges;

3) T has no cycles, and has $n - 1$ edges;

4) T is connected, but deleting any edge leaves a disconnected graph.

PROOF. We will prove that the statements are equivalent by showing that $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$. Thus, by using a sequence of implications, we see that any one of the statements implies any other.

(1 $\Rightarrow$ 2) We assume that T is a tree, and we would like to deduce that T is connected and has $n-1$ edges. By the definition of a tree, T is connected. We will use induction on n to show that T has $n-1$ edges.

Base case: $n = 1$. There is only one (unlabeled) graph on one vertex, it is K_1, so $T \cong K_1$, which has no edges. Since $0 = n - 1$, this completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 1$ be arbitrary, and suppose that every tree on k vertices has $k - 1$ edges.

Let T be an arbitrary tree with $k + 1$ vertices. Since $k + 1 \geq 2$ and T is connected, T must have at least one edge, so by Proposition 12.25, T has at least two leaves. Let v be a leaf of T. By Proposition 12.26, $T \setminus \{v\}$ is a tree. Also, $T \setminus \{v\}$ has k vertices, so we can apply our induction hypothesis to conclude that $T \setminus \{v\}$ has $k - 1$ edges. Since v was a leaf, T has precisely one more edge than $T \setminus \{v\}$, so T must have $k = (k + 1) - 1$ edges. This completes our inductive step.

By the Principle of Mathematical Induction, every tree on n vertices has $n - 1$ edges.

(2 $\Rightarrow$ 3) We assume that T is connected and has $n - 1$ edges. We need to deduce that T has no cycles.

Towards a contradiction, suppose that T has a cycle. Repeatedly delete edges that are in cycles until no cycles remain. By Proposition 12.21 (used repeatedly), the resulting graph is connected, so by definition it is a tree. Since we have already proven that $1 \Rightarrow 2$, this tree must have $n - 1$ edges. Since we started with $n - 1$ edges and deleted at least one (based on our assumption that T has at least one cycle), this is a contradiction. This contradiction serves to prove that T must not have any cycles.

(3 $\Rightarrow$ 4) We assume that T has no cycles, and has $n - 1$ edges. We must show that T is connected, and that deleting any edge leaves a disconnected graph. We begin by showing that T is connected; we prove this by induction on n.

Base case: $n = 1$. Then $T \cong K_1$ is connected.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 1$ be arbitrary, and suppose that every graph on k vertices that has $k - 1$ edges and no cycles, is connected.

Let T be an arbitrary graph with $k + 1$ vertices that has k edges and no cycles. By Euler's handshaking lemma,

$$\sum_{v \in V} d(v) = 2k.$$

If each of the $k + 1$ vertices had valency 2 or more, then we would have

$$\sum_{v \in V} d(v) \geq 2(k + 1)$$

(this is a lot like the Pigeonhole Principle in concept, but the Pigeonhole Principle itself doesn't apply to this situation). Since $2k < 2(k + 1)$, there must be some vertex v that does not have valency 2 or more. Delete v. In so doing, we delete at most 1 edge, since v has at most 1 incident edge. Thus, the resulting graph has k vertices and k or $k - 1$ edges, and since T has no cycles, neither does $T \setminus \{v\}$.

If $T \setminus \{v\}$ has k edges, then deleting any of the edges results in a graph on k vertices with no cycles and $k - 1$ edges, which by our inductive hypothesis must be connected. Therefore $T \setminus \{v\}$ is a connected graph that remains connected after any edge is deleted. By Proposition 12.24 (in the contrapositive), this means that $T \setminus \{v\}$ must contain a cycle, but this is a contradiction. This contradiction serves to prove that $T \setminus \{v\}$ cannot have k edges.

Thus, $T \setminus \{v\}$ has $k - 1$ edges and k vertices, and no cycles. By our inductive hypothesis, $T \setminus \{v\}$ must be connected. Furthermore, the fact that $T \setminus \{v\}$ has $k - 1$ edges means that v is incident to an edge, which must have its other endvertex in $T \setminus \{v\}$. Therefore T is connected. This completes the inductive step.

By the Principle of Mathematical Induction, every graph on n vertices with no cycles and $n-1$ edges is connected.

It remains to be shown that deleting any edge leaves a disconnected graph, but now that we know that T is connected, this follows from Proposition 12.24.

(4 ⇒ 1) We assume that T is connected, but deleting any edge leaves a disconnected graph. By the definition of a tree, we must show that T has no cycles. This follows immediately from Proposition 12.21. □

EXERCISES 12.28.

1) Prove Proposition 12.26.
2) Draw a tree on 6 vertices.
3) There are two non-isomorphic trees on 4 vertices. Find them.
4) There are 11 non-isomorphic graphs on 4 vertices. Draw all 11, and under each one indicate: is it connected? Is it a forest? Is it a tree?
   [*Hint:* One has 0 edges, one has 1 edge, two have 2 edges, three have 3 edges, two have 4 edges, one has 5 edges, and one has 6 edges.]

SUMMARY:

- many definitions and results about graphs can be generalised to the context of digraphs.
- Important definitions:
  - ○ digraph
  - ○ arc
  - ○ walk
  - ○ length of a walk
  - ○ connected
  - ○ connected component
  - ○ path, cycle
  - ○ tree, forest, leaf
- Notation:
  - ○ P_n
  - ○ C_n

Chapter 13

Euler and Hamilton

Some sorts of walks through a graph are particularly important for routing problems. We will be considering some of these in this chapter.

13A. Euler tours and trails

To introduce these concepts, we need to know about some special kinds of walks.

DEFINITION 13.1. A walk is **closed** if it begins and ends with the same vertex.

A **trail** is a walk in which no two vertices appear consecutively (in either order) more than once. (That is, no edge is used more than once.)

A **tour** is a closed trail.

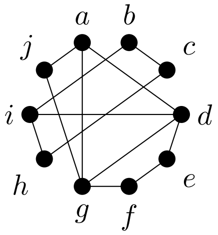
An **Euler trail** is a trail in which every pair of adjacent vertices appear consecutively. (That is, every edge is used exactly once.)

An **Euler tour** is a closed Euler trail.

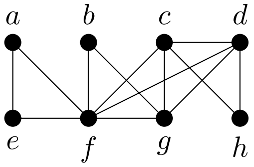
Recall the historical example of the bridges of Königsberg. The problem of finding a route that crosses every bridge exactly once, is equivalent to finding an Euler trail in the corresponding graph. If we want the route to begin and end at the same place (for example, someone's home), then the problem is equivalent to finding an Euler tour in the corresponding graph.

Euler tours and trails are important tools for planning routes for tasks like garbage collection, street sweeping, and searches.

EXAMPLE 13.2. In the graph



$(i, b, c, h, i, d, e, f, g, d, a, g, j, a)$ is an Euler trail. In the graph



$(a, e, f, b, g, f, c, d, h, c, g, d, f, a)$ is an Euler tour.

Here is Euler's method for finding Euler tours. We will state it for multigraphs, as that makes the corresponding result about Euler trails a very easy corollary.

THEOREM 13.3. *A connected graph (or multigraph, with or without loops) has an Euler tour if and only if every vertex in the graph has even valency.*

PROOF. As the statement is if and only if, we must prove both implications.

(⇒) Suppose we have a multigraph (possibly with loops) that has an Euler tour,

$$(u_1, u_2, \dots, u_{e+1} = u_1),$$

where $e = |E|$. Let u be an arbitrary vertex of the multigraph. Every time u appears in the tour, exactly two of the edges incident with u are used: if $u = u_j$, then the edges used are $u_{j-1}u_j$ and u_ju_{j-1} unless $j = 1$ or $j = e+1$ in which case $u = u_1 = u_{e+1}$ and the edges are u_eu and uu_2 (and we consider this as one appearance of u in the tour). Therefore, if u appears k times in the tour, then since by the definition of an Euler tour all edges incident with u are used exactly once, we conclude that u must have valency $2k$. Since u was an arbitrary vertex of the multigraph and k (the number of times u appears in the tour) must be an integer, this shows that the valency of every vertex must be even.

(⇐) Suppose we have a connected multigraph in which the valency of every vertex is even. Consider the following algorithm (which will be the first stage of our final algorithm):

Make u (some arbitrary vertex) our active vertex, with a list L of all of the edges of E. Make u the first vertex in a new sequence C of vertices. Repeat the following step as many times as possible:

Call the active vertex v. Choose any edge vx in L that is incident with v. Add x (the other endvertex of this edge) to the end of C, and make x the new active vertex. Remove vx from L.

We claim that when this algorithm terminates, the sequence C will be a tour (though not necessarily an Euler tour) in the multigraph. By construction, C is a walk, and C cannot use any edge more than once since each edge appears in L only once and is removed from L once it has been used, so C is a trail. We need to show that the walk C is closed.

The only way the algorithm can terminate is if L contains no edge that is incident with the active vertex. Towards a contradiction, suppose that this happens at a time when the active vertex is $y \neq u$. Now, y has valency $2r$ in the multigraph for some integer r, so there were $2r$ edges in L that were incident with y when we started the algorithm. Since $y \neq u$, every time y appears in C before this appearance, we removed 2 edges incident with y from L (one in the step when we made y the active vertex, and one in the following step). Furthermore, we removed one additional edge incident with y from L in the final step, when we made y the active vertex again. Thus if there are t previous appearances of y in C, we have removed $2t+1$ edges incident with y from L. Since $2r$ is even and $2t+1$ is odd, there must still be at least one edge incident with y that is in L, contradicting the fact that the algorithm terminated. This contradiction shows that, when the algorithm terminates, the active vertex must be u, so the sequence C is a closed walk. Since C is a trail, we see that C must be a tour.

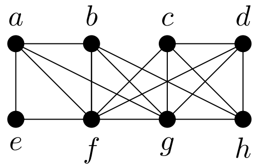
If the tour C is not an Euler tour, let y be the first vertex that appears in C for which there remains an incident edge in L. Repeat the previous algorithm starting with y being the active vertex, and with L starting at its current state (not all of E). The result will be a tour beginning and ending at y that uses only edges that were not in C. Insert this tour into C as follows: if $C = (u = u_1 \dots, y = u_i, \dots, u_k = u)$ and the new tour is $(y = v_1, \dots, v_j = y)$, then the result of inserting the new tour into C will be

$$(u = u_1, \dots, y = u_i = v_1, v_2, \dots, v_j = y = u_i, u_{i+1}, \dots, u_k = u).$$

Replace C by this extended tour.

Repeat the process described in the previous paragraph as many times as possible (this is the second and last stage of our final algorithm). Since E is finite and the multigraph is connected, sooner or later all of the edges of L must be exhausted. At this point, we must have an Euler tour. □

EXAMPLE 13.4. Use the algorithm described in the proof of the previous result, to find an Euler tour in the following graph.



SOLUTION. Let's begin the algorithm at a. As $E = L$ is a large set, we won't list the remaining elements every time we choose a new active vertex in the early stages. An easy method for you to keep track of the edges still in L is to colour the edges that are no longer in L (the edges we use) with a different colour as we go.

There are many different possible outcomes for the algorithm since there are often many acceptable choices for the next active vertex. One initial set of choices could be

$$C = (a, b, f, e, a, f, g, a).$$

The first stage of the algorithm terminates at this point since all four edges incident with a have been used. At this point, we have

$$L = \{bg, bh, cd, cf, cg, ch, df, dg, dh, gh\}.$$

The first vertex in C that is incident with an edge in L is b. We run the first stage of the algorithm again with b as the initial active vertex and this list for L. Again, there are many possible outcomes; one is (b, g, h, b).

We insert (b, g, h, b) into C, obtaining a new $C = (a, b, g, h, b, f, e, a, f, g, a)$. At this point, we have

$$L = \{cd, cf, cg, ch, df, dg, dh\}.$$

Now g is the first vertex in C that is incident with an edge in L. We run the first stage of the algorithm again with g as the initial active vertex and the current L. One possible outcome is (g, c, f, d, g).

Inserting this into C yields a new

$$C = (a, b, g, c, f, d, g, h, b, f, e, a, f, g, a).$$

At this point, we have $L = \{cd, ch, dh\}$. The first vertex in C that is incident with an edge in L is c. We run the first stage of the algorithm one final time with c as the initial active vertex and $L = \{cd, ch, dh\}$. This time there are only two possible outcomes: (c, d, h, c) or (c, h, d, c). We choose (c, d, h, c).

Inserting this into C yields our Euler tour:

$$C = (a, b, g, c, d, h, c, f, d, g, h, b, f, e, a, f, g, a).$$ □

COROLLARY 13.5. *A connected graph (or multigraph, with or without loops) has an Euler trail if and only if at most two vertices have odd valency.*

PROOF. Suppose we have a connected graph (or multigraph, with or without loops), G. Since the statement is if and only if, there are two implications to prove.

(⇒) Suppose that G has an Euler trail. If the trail is closed then it is a tour, and by Theorem 13.3, there are no vertices of odd valency. If the trail is not closed, say it is a $u - v$ walk. Add an edge between u and v to G, creating a new graph G^* (note that G^* may be a multigraph if uv was already an edge of G, even if G wasn't a multigraph), and add u to the end of the Euler trail in G, to create an Euler tour in G^*. By Theorem 13.3, the fact that G^* has an Euler tour means that every vertex of G^* has even valency. Now, the vertices of G all have the same valency in G^* as they have in G, with the exception that the valencies of u and v are one higher in G^* than in G. Therefore, in this case there are exactly two vertices of odd valency in G; namely, u and v.

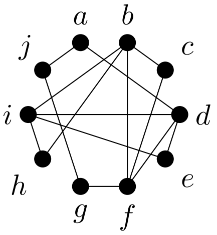
(⇐) Now we suppose that G has at most 2 vertices of odd valency. By Corollary 11.21 (the corollary to Euler's handshaking lemma), if there are at most two vertices of odd valency, then there are either 0 or 2 vertices of odd valency. We consider these two cases.

If there are 0 vertices of odd valency, then by Theorem 13.3, G has an Euler tour.

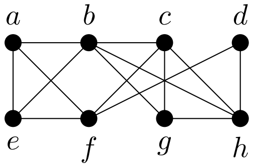
If there are two vertices of odd valency, say u and v, add an edge between u and v to G, creating a new graph G^* (note that G^* may be a multigraph if uv was already an edge of G, even if G wasn't a multigraph). Now in G^* every vertex has even valency, so G^* has an Euler tour. In fact, a careful look at the algorithm given in the proof of Theorem 13.3 shows that we may choose u and v (in that order) to be the first two vertices in this Euler tour, so that uv (the edge that is in G^* but not G) is the first edge used in the tour. Now if we delete u from the start of this Euler tour, the result is an Euler trail in G that starts at v and ends at u. □

EXERCISES 13.6. For each of the following graphs, is there an Euler tour? Is there an Euler trail? If either exists, find one; if not, explain why not.

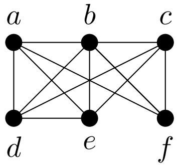
1)



2)



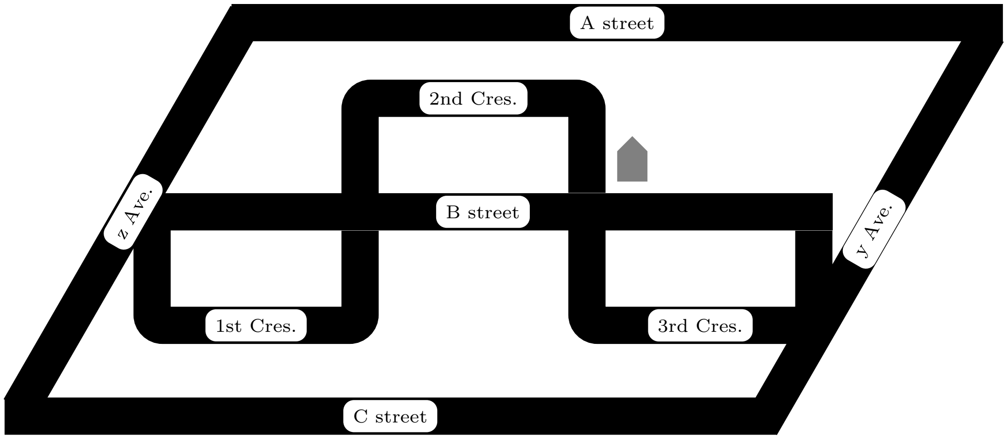
3)



4) If it is possible, draw a graph that has an even number of vertices and an odd number of edges, that also has an Euler tour. If that isn't possible, explain why there is no such graph.

5) Which complete graphs have an Euler tour? Of the complete graphs that do not have an Euler tour, which of them have an Euler trail?

EXERCISES 13.7. Sylvia's cat is missing. She wants to look for it in all the nearby streets, but she is tired and doesn't want to walk any farther than she must. Find an efficient route for Sylvia to take through her neighbourhood so that she starts and ends at home and walks through each street exactly once. The location of Sylvia's house is marked with a house-shaped symbol (⌂).



13B. Hamilton paths and cycles

Sometimes, rather than traveled along every connection in a network, our object is simply to visit every node of the network. This relates to a different structure in the corresponding graph.

DEFINITION 13.8. A **Hamilton cycle** is a cycle that visits *every* vertex of the graph.

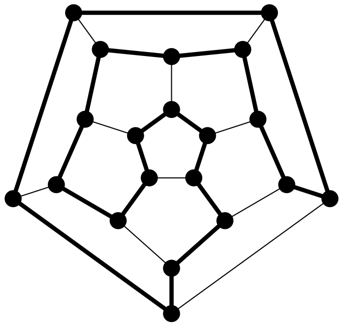
A **Hamilton path** is a path that visits *every* vertex of the graph.

The definitions of path and cycle ensure that vertices are not repeated. Hamilton paths and cycles are important tools for planning routes for tasks like package delivery, where the important point is not the routes taken, but the places that have been visited.

In 1857, William Rowan Hamilton first presented a game he called the "icosian game." It involved tracing edges of a dodecahedron in such a way as to visit each corner precisely once. In fact, two years earlier Reverend Thomas Kirkman had sent a paper to the Royal Society in London, in which he posed the problem of finding what he called *closed polygons* in polyhedra; a closed polygon he defined as a circuit of edges that passes through each vertex just once. Thus, Kirkman had posed a more general problem prior to Hamilton (and made some progress toward solving it); nonetheless, it is Hamilton for whom these structures are now named. As we'll see later when studying Steiner Triple Systems in design theory, Kirkman was a gifted mathematician who seems to have been singularly unlucky in terms of receiving proper credit for his achievements. As his title indicates, Kirkman was a minister who pursued mathematics on the side, as a personal passion.

Hamilton managed to convince the company of John Jacques and sons, who were manufacturers of toys (including high-quality chess sets) to produce and market the "icosian game." It was produced under the name *Around the World*, and sold in two forms: a flat board, or an actual dodecahedron. In both cases, nails were placed at the corners of the dodecahedron representing cities, and the game was played by wrapping a string around the nails, traveled only along edges, visiting each nail once, and ending at the starting point. Unfortunately, the game was not a financial success. It is not very difficult and becomes uninteresting once solved.

The thick edges form a Hamilton cycle in the graph of the dodecahedron:



Not every connected graph has a Hamilton cycle; in fact, not every connected graph has a Hamilton path.

Figure 13.1. A graph with a Hamilton path but no Hamilton cycle

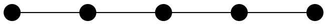
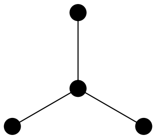


Figure 13.2. A graph with no Hamilton path



Unfortunately, in contrast to Euler's result about Euler tours and trails (given in Theorem 13.3 and Corollary 13.5), there is no known characterisation that enables us to quickly determine whether or not an arbitrary graph has a Hamilton cycle (or path). This is a hard problem in general. We do know of some necessary conditions (any graph that fails to meet these conditions cannot have a Hamilton cycle) and some sufficient conditions (any graph that meets these must have a Hamilton cycle). However, many graphs fail to meet any of these conditions. There are also some conditions that are either necessary or sufficient for the existence of a Hamilton path.

Here is a necessary condition for a graph to have a Hamilton cycle.

THEOREM 13.9. *If G is a graph with a Hamilton cycle, then for every $S \subset V$ with $S \neq \emptyset, V$, the graph $G \setminus S$ has at most $|S|$ connected components.*

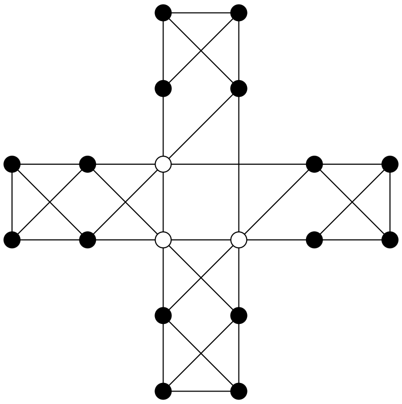
PROOF. Let C be a Hamilton cycle in G. Fix an arbitrary proper, nonempty subset S of V.

One at a time, delete the vertices of S from C. After the first vertex is deleted, the result is still connected, but has become a path. When any of the subsequent $|S| - 1$ vertices is deleted, it either breaks some path into two shorter paths (increasing the number of connected components by one) or removes a vertex at an end of some path (leaving the number of connected components unchanged, or reducing it by one if this component was a P_0). So $C \setminus S$ has at most $1 + (|S| - 1) = |S|$ connected components.

Notice that if two vertices u and v are in the same connected component of $C \setminus S$, then they will also be in the same connected component of $G \setminus S$. This is because adding edges can only connect things more fully, reducing the number of connected components. More formally, if there is a $u - v$ walk in C, then any pair of consecutive vertices in that walk is adjacent in C so is also adjacent in G. Therefore the same walk is a $u - v$ walk in G. This tells us that the number of connected components of $G \setminus S$ is at most the number of connected components of $C \setminus S$, which we have shown to be at most $|S|$. □

EXAMPLE 13.10. When a non-leaf is deleted from a path of length at least 2, the deletion of this single vertex leaves two connected components. So no path of length at least 2 contains a Hamilton cycle.

Here's a graph in which the non-existence of a Hamilton cycle might be less obvious without Theorem 13.9. Deleting the three white vertices leaves four connected components.



As you might expect, if all of the vertices of a graph have sufficiently high valency, it will always be possible to find a Hamilton cycle in the graph. (In fact, generally the graph will have many different Hamilton cycles.) Before we can formalise this idea, it is helpful to have an additional piece of notation.

DEFINITION 13.11. The **minimum valency** of a graph G is

$$\min_{v \in V} d(v).$$

The **maximum valency** of a graph G is

$$\max_{v \in V} d(v).$$

NOTATION 13.12. We use δ to denote the minimum valency of a graph, and Δ to denote its maximum valency. If we need to clarify the graph involved, we use $\delta(G)$ or $\Delta(G)$.

Although the following theorem was proven back in 1952, it remains one of the most powerful known methods for determining that a graph has a Hamilton cycle.

THEOREM 13.13 (Dirac, 1952). *If G is a graph with vertex set V such that $|V| \geq 3$ and $\delta(G) \geq |V|/2$, then G has a Hamilton cycle.*

PROOF. Towards a contradiction, suppose that G is a graph with vertex set V, that $|V| = n \geq 3$, and that $\delta(G) \geq n/2$, but G has no Hamilton cycle.

Repeat the following as many times as possible: if there is an edge that can be added to G without creating a Hamilton cycle in the resulting graph, add that edge to G. When this has been done as many times as possible, call the resulting graph H. The graph H has the same vertex set V, and since we have added edges we have not decreased the valency of any vertex, so we have $\delta(H) \geq n/2$. Now, H still has no Hamilton cycle, but adding any edge to H gives a graph that does have a Hamilton cycle.

Since complete graphs on at least three vertices always have Hamilton cycles (see Exercise 13.19(1)), we must have $H \not\cong K_n$, so there are at least two vertices of H, say u and v, that are not adjacent. By our construction of H from G, adding the edge uv to H would result in a Hamilton cycle, and this Hamilton cycle must use the edge uv (otherwise it would be a Hamilton cycle in H, but H has no Hamilton cycle). Thus, the portion of the Hamilton cycle that is in H forms a Hamilton path from u to v. Write this Hamilton path as

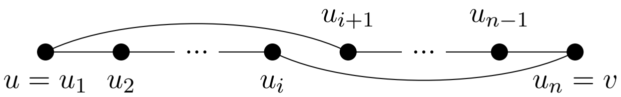
$$(u = u_1, u_2, \ldots, u_n = v).$$

Define the sets

$$S = \{u_i \mid u \sim u_{i+1}\} \text{ and } T = \{u_i \mid v \sim u_i\}.$$

That is, S is the set of vertices that appear immediately before a neighbour of u on the Hamilton path, while T is the set of vertices on the Hamilton path that are neighbours of v. Notice that $v = u_n \notin S$ since u_{n+1} isn't defined, and $v = u_n \notin T$ since our graphs are simple (so have no loops). Thus, $u_n \notin S \cup T$, so $|S \cup T| < n$.

Towards a contradiction, suppose that for some i, $u_i \in S \cap T$. Then by the definitions of S and T, we have $u \sim u_{i+1}$ and $v \sim u_i$, so:



is a Hamilton cycle in H, which contradicts our construction of H as a graph that has no Hamilton cycle. This contradiction serves to prove that $|S \cap T| = \emptyset$.

Now we have

$$d_H(u) + d_H(v) = |S| + |T| = |S \cup T| + |S \cap T|$$

(the last equality comes from Inclusion-Exclusion). But we have seen that $|S \cup T| < n$ and $|S \cap T| = 0$, so this gives

$$d_H(u) + d_H(v) < n.$$

This contradicts $\delta(H) \geq n/2$, since

$$d_H(u), d_H(v) \geq \delta(H).$$

This contradiction serves to prove that no graph G with vertex set V such that $|V| \geq 3$ and $\delta(G) \geq |V|/2$ can fail to have a Hamilton cycle. □

In fact, the statement of Dirac's theorem was improved by Bondy and Chvatal in 1974. They began by observing that the proof given above for Dirac's Theorem actually proves the following result.

LEMMA 13.14. *Suppose that G is a graph on n vertices, u and v are nonadjacent vertices of G, and $d(u) + d(v) \geq n$. Then G has a Hamilton cycle if and only if the graph obtained by adding the edge uv to G has a Hamilton cycle.*

With this in mind, they made the following definition.

DEFINITION 13.15. Let G be a graph on n vertices. The **closure** of G is the graph obtained by repeatedly joining pairs of nonadjacent vertices u and v for which $d(u) + d(v) \geq n$, until no such pair exists.

Before they were able to work with this definition, they had to prove that the closure of a graph is well-defined. In other words, since there will often be choices involved in forming the closure of a graph (if more than one pair of vertices satisfy the condition, which edge do we add first?), is it possible that by making different choices, we might end up with a different graph at the end? The answer, fortunately, is no; any graph has a unique closure, as we will now prove.

LEMMA 13.16. *Closure is well-defined. That is, any graph has a unique closure.*

PROOF. Let $(e_1, \dots, e_\ell)$ be one sequence of edges we can choose to arrive at the closure of G, and let the resulting closure be the graph G_1. Let $(f_1, \dots, f_m)$ be another such sequence, and let the resulting closure be the graph G_2. We will prove by induction on ℓ that for every $1 \le i \le \ell$, $e_i \in \{f_1, \dots, f_m\}$. We will use $\{u_i, v_i\}$ to denote the endvertices of e_i.

Base case: $\ell = 1$, so only the edge $\{u_1, v_1\}$ is added to G in order to form G_1. Since this was the first edge added, we must have

$$d_G(u_1) + d_G(v_1) \ge n.$$

Since G_2 has all of the edges of G, we must certainly have

$$d_{G_2}(u_1) + d_{G_2}(v_1) \ge n.$$

Since G_2 is a closure of G, it has no pair of nonadjacent edges whose valencies sum to n or higher, so u_1 must be adjacent to v_1 in G_2. Since the edge u_1v_1 was not in G, it must be in $\{f_1, \dots, f_m\}$. This completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $k \ge 1$ be arbitrary (with $k \le \ell$), and suppose that

$$e_1, \dots, e_k \in \{f_1, \dots, f_m\}.$$

Consider $e_{k+1} = \{u_{k+1}, v_{k+1}\}$. Let G' be the graph obtained by adding the edges $e_1, \dots, e_k$ to G. Since e_{k+1} was chosen to add to G' to form G_1, it must be the case that

$$d_{G'}(u_{k+1}) + d_{G'}(v_{k+1}) \ge n.$$

By our induction hypothesis, all of the edges of G' are also in G_2, so this means

$$d_{G_2}(u_{k+1}) + d_{G_2}(v_{k+1}) \ge n.$$

Since G_2 is a closure of G, it has no pair of nonadjacent edges whose valencies sum to n or higher, so u_{k+1} must be adjacent to v_{k+1} in G_2. Since the edge e_{k+1} was not in G, it must be in $\{f_1, \dots, f_m\}$.

By the Principle of Mathematical Induction, G_2 contains all of the edges of G_1. Since there was nothing special about G_2 as distinct from G_1, we could use the same proof to show that G_1 contains all of the edges of G_2. Therefore, G_1 and G_2 have the same edges. Since they also have the same vertices (the vertices of G), they are the same graph. Thus, the closure of any graph is unique. □

This allowed Bondy and Chvatal to deduce the following result, which is stronger than Dirac's although as we've seen the proof is not significantly different.

THEOREM 13.17. *A simple graph has a Hamilton cycle if and only if its closure has a Hamilton cycle.*

PROOF. Repeatedly apply Lemma 13.14. □

This has a very nice corollary.

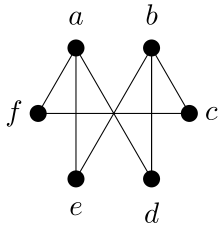
COROLLARY 13.18. *A simple graph on at least 3 vertices whose closure is complete, has a Hamilton cycle.*

PROOF. This is an immediate consequence of Theorem 13.17 together with the fact (see Exercise 13.19(1)) that every complete graph on at least 3 vertices has a Hamilton cycle. □

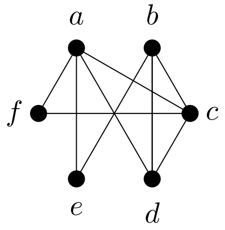
EXERCISES 13.19.

1) Prove by induction that for every $n \geq 3$, K_n has a Hamilton cycle.
2) Find the closure of each of these graphs. Can you easily tell from the closure whether or not the graph has a Hamilton cycle?

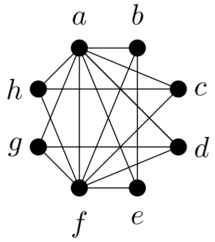
(a)



(b)



3) Use Theorem 13.9 to prove that this graph does not have a Hamilton cycle.



4) Prove that if G has a Hamilton path, then for every nonempty proper subset S of V, $G - S$ has no more than $|S| + 1$ connected components.
5) For the two graphs in Exercise 13.19(2), either find a Hamilton cycle or use Theorem 13.9 to show that no Hamilton cycle exists.

SUMMARY:

- algorithms for finding Euler tours and trails
- Important definitions:
  - closed walk, trail, tour
  - Euler tour, Euler trail
  - Hamilton cycle, Hamilton path
  - minimum valency, maximum valency
  - closure of a graph
- Notation:
  - δ, Δ

Chapter 14

Graph Colouring

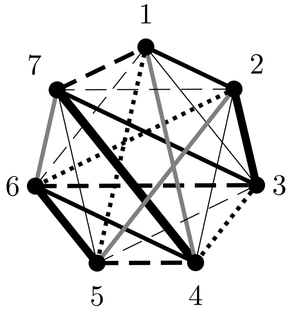
14A. Edge colouring

Suppose you have been given the job of scheduling a round-robin tennis tournament with n players. One way to approach the problem is to model it as a graph: the vertices of the graph will represent the players, and the edges will represent the matches that need to be played. Since it is a round-robin tournament, every player must play every other player, so the graph will be complete. Creating the schedule amounts to assigning a time to each of the edges, representing the time at which that match is to be played.

Notice that there is a constraint. When you have assigned a time to a particular edge uv, no other edge incident with either u or v can be assigned the same time, since this would mean that either player u or player v is supposed to play two games at once. Instead of writing times on each edge, we will choose a colour to represent each of the time slots, and colour the edges that are to be played at that time, with that colour.

Here is an example of a possible schedule for the tournament, when $n = 7$.

EXAMPLE 14.1. The players are numbered from 1 through 7, and we will spread the tournament out over seven days. Games to be played on each day should have a different colour than the games on other days, but, because this text is printed in black-and-white, we will use some line patterns, instead of colours. Games to be played on Monday will be drawn as usual. Games to be played on Tuesday will be thin. Games to be played on Wednesday will be dotted. Games to be played on Thursday will be dashed. Games to be played on Friday will be thick. Games to be played on Saturday will be grey. Games to be played on Sunday will be thin and dashed.



This gives a schedule. For anyone who has trouble distinguishing the "colours" of the edges, the normal edges are 12, 37, and 46; the thin edges are 13, 24, and 57; the dotted edges are 15, 26, and 34; the dashed edges are 17, 36, and 45; the thick edges are 23, 47, and 56; the grey edges are 14, 25, and 67; and the thin dashed edges are 16, 27, and 35.

DEFINITION 14.2. A **proper k-edge-colouring** of a graph G is a function that assigns to each edge of G one of k colours, such that edges that meet at an endvertex must be assigned different colours.

The constraint that edges of the same colour cannot meet at a vertex turns out to be a useful constraint in a number of contexts.

If the graph is large enough we are liable to run out of colours that can be easily distinguished (and we get tired of writing out the names of colours). The usual convention is to refer to each colour by a number (the first colour is colour 1, etc.) and to label the edges with the numbers rather than using colours.

DEFINITION 14.3. A graph G is **k-edge-colourable** if it admits a proper k-edge-colouring. The smallest integer k for which G is k-edge-colourable is called the **edge chromatic number**, or **chromatic index** of G.

NOTATION 14.4. The chromatic index of G is denoted by $\chi'(G)$, or simply by χ' if the context is unambiguous.

Here is an easy observation:

PROPOSITION 14.5. *For any graph G, $\chi'(G) \geq \Delta(G)$.*

PROOF. Recall that $\Delta(G)$ denotes the maximum value of $d(v)$ over all vertices v of G. So there is some vertex v of G such that $d(v) = \Delta(G)$. In any proper edge-colouring, the $d(v)$ edges that are incident with v, must all be assigned different colours. Thus, any proper edge-colouring must have at least $d(v) = \Delta(G)$ distinct colours. This means $\chi'(G) \geq \Delta(G)$. □

EXAMPLE 14.6. The colouring given in Example 14.1 shows that $\chi'(K_7) \leq 7$, since we were able to properly edge-colour K_7 using seven colours.

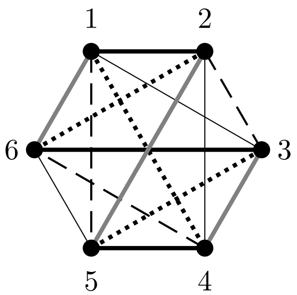
To show that we cannot colour K_7 with fewer than 7 colours, notice that because each of the 7 vertices can only be incident with one edge of a given colour, there cannot be more than 3 edges coloured with any given colour (3 edges are already incident with 6 of the 7 vertices, and a fourth edge would have to be incident with two others).

We know that K_7 has $\binom{7}{2} = 21$ edges, so if at most 3 edges can be coloured with any given colour, we will require at least 7 colours to properly edge-colour K_7. Thus $\chi'(K_7) \geq 7$.

Thus, we have shown that $\chi'(K_7) = 7$.

This shows that $\chi'(K_7) = 7 > \Delta(K_7) = 6$, so it is not always possible to achieve equality in the bound given by Proposition 14.5. Our next example shows that it *is* sometimes possible to achieve equality in that bound.

EXAMPLE 14.7. Here is a proper 5-edge-colouring of K_6:



In case the edge colours are difficult to distinguish, the thick edges are 12, 36, and 45; the thin edges are 13, 24, and 56; the dotted edges are 14, 26, and 35; the dashed edges are 15, 23, and 46; and the grey edges are 16, 25, and 34. This shows that $\chi'(K_6) \le 5$. Since the valency of every vertex of K_6 is 5, Proposition 14.5 implies that $\chi'(K_6) \ge 5$. Putting these together, we see that $\chi'(K_6) = \Delta(K_6) = 5$, so equality in the bound of Proposition 14.5 is achieved by K_6.

The following rather remarkable result was proven by Vadim Vizing in 1964:

THEOREM 14.8. Vizing's Theorem *For any simple graph G, $\chi'(G) \in \{\Delta(G), \Delta(G)+1\}$.*

We will not go over the proof of this theorem.

DEFINITION 14.9. If $\chi'(G) = \Delta(G)$ then G is said to be a **class one graph**, and if $\chi'(G) = \Delta(G) + 1$ then G is said to be a **class two graph**.

To date, graphs have not been completely classified according to which graphs are class one and which are class two, but it has been proven that "almost every" graph is of class one. Technically, this means that if you choose a random graph out of all of the graphs on at most n vertices, the probability that you will choose a class two graph approaches 0 as n approaches infinity.

There are, however, infinitely many class two graphs; the same argument we used to show that $\chi'(K_7) \ge 7$ can also be used to prove that $\chi'(K_{2n+1}) = 2n+1$ for any positive integer n, since the number of edges is

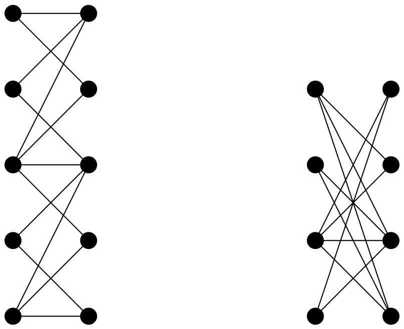
$$(2n+1)(2n)/2 = n(2n+1)$$

and each colour can only be used to colour n of the edges. Since $\Delta(K_{2n+1}) = 2n$, this shows that K_{2n+1} is class two.

Large families of graphs have been shown to be class one graphs. We will devote most of the rest of this section to proving that all of the graphs in one particular family are class one. First we need to define the family.

DEFINITION 14.10. A graph is **bipartite** if its vertices can be partitioned into two sets V_1 and V_2, such that every edge of the graph has one of its endvertices in V_1, and the other in V_2. The sets V_1 and V_2 form a **bipartition** of the graph.

EXAMPLE 14.11. The following graphs are bipartite. Every edge has one endvertex on the left side, and one on the right.



The graph K_n is not bipartite if $n \ge 3$. The first vertex may as well go into V_1; the second vertex is adjacent to it, so must go into V_2; but the third vertex is adjacent to both, so cannot go into either V_1 or V_2.

Although the following class of bipartite graphs will not be used in this chapter, they are an important class of bipartite graphs that will come up again later.

DEFINITION 14.12. The **complete bipartite graph**, $K_{m,n}$, is the bipartite graph on $m+n$ vertices with as many edges as possible subject to the constraint that it has a bipartition into sets of cardinality m and n. That is, it has every edge between the two sets of the bipartition.

Before proving that all bipartite graphs are class one, we need to understand the structure of bipartite graphs a bit better. Here is an important theorem.

THEOREM 14.13. *A graph G is bipartite if and only if G contains no cycle of odd length.*

PROOF. This is an if and only if statement, so we have two implications to prove.

(⇒) We prove the contrapositive, that if G contains a cycle of odd length, then G cannot be bipartite.

Let

$$(v_1, v_2, \dots, v_{2k+1}, v_1)$$

be a cycle of odd length in G. We try to establish a bipartition V_1 and V_2 for G. Without loss of generality, we may assume that $v_1 \in V_1$. Then we must have $v_2 \in V_2$ since $v_2 \sim v_1$. Continuing in this fashion around the cycle, we see that for every $1 \leq i \leq k$, we have $v_{2i+1} \in V_1$ and $v_{2i} \in V_2$. In particular, $v_{2k+1} \in V_1$, but $v_1 \in V_1$ and $v_1 \sim v_{2k+1}$, contradicting the fact that every edge must have one of its endvertices in V_2. Thus, G is not bipartite.

(⇐) Let G be a graph that is not bipartite. We must show that there is an odd cycle in G.

If every connected component of G is bipartite, then G is bipartite (choose one set of the bipartition from each connected component; let V_1 be the union of these, and V_2 the set of all other vertices of G; this is a bipartition for G). Thus there is at least one connected component of G that is not bipartite.

Pick any vertex u from a non-bipartite connected component of G, and assign it to V_1. Place all of its neighbours in V_2. Place all of their neighbours into V_1. Repeat this process, at each step putting all of the neighbours of every vertex of V_1 into V_2, and then all of the neighbours of every vertex of V_2 into V_1.

Since this component is not bipartite, at some point we must run into the situation that we place a vertex v into V_j, but a neighbour u_1 of v is also in V_j (for some $j \in \{1, 2\}$). By our construction of V_1 and V_2, there must be a walk from u_1 to v that alternates between vertices in V_j and vertices in V_{3-j}. By Proposition 12.16, there must in fact be a *path* from u_1 to v that alternates between vertices in V_j and vertices in V_{3-j}. Since the path alternates between the two sets but begins and ends in V_j, it has even length. Therefore, adding u_1 to the end of this path yields a cycle of odd length in G. □

In order to prove that bipartite graphs are class one, we require a lemma.

LEMMA 14.14. *Let G be a connected graph that is not a cycle of odd length. Then G the edges of G can be 2-coloured so that edges of both colours are incident with every non-leaf vertex. (Note: this will probably not be a* proper *2-edge-colouring of G.)*

PROOF. We first consider the case where every vertex of G has even valency.

Choose a vertex v of G subject to the constraint that if any vertex of G has valency greater than 2, then v is such a vertex. Since every vertex of G has even valency, we can find an Euler tour of G that begins and ends at v. Alternate edge colours around this tour. Clearly, every vertex that is visited in the middle of the tour (that is, every vertex except possibly v) must be incident with edges of both colours, since whichever colour is given to the edge we travel to reach that vertex, the other colour will be given to the edge we travel when leaving that vertex. If any vertex of G has valency greater than 2, then by our choice of v, the valency of v must be greater than 2, so v is visited in the middle of the tour, and this colouring has the desired property. If every vertex of G has valency 2, then since G is connected, G must be a cycle (see Exercise 12.22(4). Since G is not a cycle of odd length (by hypothesis), G must be a cycle of even length. Therefore the number of edges of G is even, so the tour will begin and end with edges of opposite colours, both of which are incident with v. Again we see that this colouring has the desired property.

Suppose now that G has at least one vertex of odd valency.

Create a new vertex, u, and add edges between u and every vertex of G that has odd valency. All of the vertices of G will have even valency in this new graph, and by the corollary to Euler's handshaking lemma, u must also have even valency, so this graph has an Euler tour; in fact, we can find an Euler tour that begins with the vertex u. Alternate edge colours around this tour. Delete u (and its incident edges) but retain the colours on the edge of G. We claim that this colouring will have the desired property. If a vertex v has even valency in G, it must be visited in the middle of the tour and the edges we travel on to reach v and to leave v will have different colours. Neither of these edges is incident with u, so both are in G. If a vertex v has valency 1 in G, then v is a leaf and the colour of its incident edge doesn't matter. If a vertex v has odd valency at least 3 in G, then v is visited at least twice in the middle of the tour. Only one of these visits can involve the edge uv, so during any other visit, the edges we travel on to reach v and to leave v will have different colours. Neither of these edges is incident with u, so both are in G. Thus, this colouring has the desired property. □

NOTATION 14.15. Given a (not necessarily proper) edge-colouring $\mathcal{C}$, we use $c(v)$ to denote the number of distinct colours that have be used on edges that are incident with v. Clearly, $c(v) \leq d(v)$.

DEFINITION 14.16. An edge colouring $\mathcal{C}'$ is an **improvement** on an edge colouring $\mathcal{C}$ if it uses the same colours as $\mathcal{C}$, but $\sum_{v \in V} c'(v) > \sum_{v \in V} c(v)$.

An edge colouring is **optimal** if no improvement is possible.

Notice that since $c(v) \leq d(v)$ for every $v \in V$, if

$$\sum_{v \in V} c(v) = \sum_{v \in V} d(v)$$

then we must have $c(v) = d(v)$ for every $v \in V$. This is precisely equivalent to the definition of a proper colouring.

At last, we are ready to prove that bipartite graphs are class one.

THEOREM 14.17. *If G is bipartite, then $\chi'(G) = \Delta(G)$.*

PROOF. Let G be a bipartite graph. Towards a contradiction, suppose that $\chi'(G) > \Delta(G)$.

Let $\mathcal{C}$ be an optimal $\Delta(G)$-edge-colouring of G. By assumption, $\mathcal{C}$ will not be a proper edge colouring, so there must be some vertex u such that $c(u) < d(u)$. By the Pigeonhole Principle, some colour j must be used to colour at least two of the edges incident with u, and since there are $\Delta(G) \geq d(u)$ colours in total and only $c(u)$ are used on edges incident with u, there must be some colour i that is not used to colour any edge incident with u.

Consider only the edges of G that have been coloured with either i or j in the colouring $\mathcal{C}$. Since G is bipartite, these edges cannot include an odd cycle. We apply Lemma 14.14 to each connected component formed by these edges to re-colour these edges . Our re-colouring will use only colours i and j, and if a vertex v was incident to at least two edges coloured with either i or j in $\mathcal{C}$, then under the re-colouring, v will be incident with at least one edge coloured with i and at least one edge coloured with j. Leave all of the other edge colours alone, and call this new colouring $\mathcal{C}'$.

We claim that $\mathcal{C}'$ is an improvement on $\mathcal{C}$. Any vertex v that had at most one incident edge coloured with either i or j under $\mathcal{C}$, will still have exactly the same colours except that the edge coloured i or j might have switched its colour to the other of i and j. In any case, we will have $c'(v) = c(v)$. Any vertex v that had at least two incident edges coloured with either i or j under $\mathcal{C}$, will still have all of the same colours except that it will now have incident edges coloured with both i and j, so $c'(v) \geq c(v)$. Furthermore, we have $c'(u) > c(u)$ since the edges incident with u now include edges coloured with both i and j, where before there were only edges coloured with j. Thus,

$$\sum_{v \in V} c'(v) \geq \sum_{v \in V} c(v),$$

so $\mathcal{C}'$ is an improvement on $\mathcal{C}$, as claimed.

We have contradicted our assumption that $\mathcal{C}$ is an optimal $\Delta(G)$-edge-colouring. This contradiction serves to prove that $\chi'(G) = \Delta(G)$. □

EXERCISES 14.18.

1) Prove that every tree is a class one graph.

2) Prove that every cycle of odd length is a class two graph.

3) Find a graph that contains a cycle of odd length, but is a class one graph.

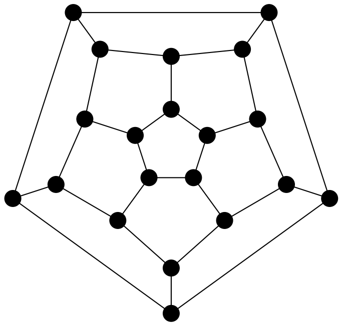
4) For each of the following graphs, find the edge-chromatic number, determine whether the graph is class one or class two, and find a proper edge-colouring that uses the smallest possible number of colours.

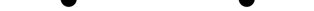
   (a) The two graphs in Exercise 13.19(2).

   (b) The two graphs in Example 14.11.

   (c) The skeleton of a dodecahedron (the leftmost of the two graphs drawn below).

   (d) The *Petersen graph* (the rightmost of the two graphs drawn below).
   You may assume, without proof, that the Petersen graph is class two.





5) Find a systematic approach to colouring the edges of complete graphs that demonstrates that $\chi'(K_{2n-1}) = \chi'(K_{2n}) = 2n - 1$.

6) Find a systematic approach to colouring the edges of complete bipartite graphs that demonstrates that $\chi'(K_{m,n}) = \Delta(K_{m,n}) = \max\{m, n\}$.

EXERCISES 14.19. The following exercises illustrate some of the connections between Hamilton cycles and edge-colouring.

1) **Definition.** A graph is said to be *Hamilton-connected* if there is a Hamilton path from each vertex in the graph to each of the other vertices in the graph.

   Prove that if G is bipartite and has at least 3 vertices, then G is not Hamilton-connected.

   [*Hint:* Prove this by contradiction. Consider the length of a Hamilton path and where it can end.]

2) Suppose that G is a bipartite graph with V_1 and V_2 forming a bipartition. Show that if $|V_1| \neq |V_2|$ then G has no Hamilton cycle.

3) Prove that if every vertex of G has valency 3, and G has a Hamilton cycle, then G is class one.
   [*Hint:* Use the corollary to Euler's handshaking lemma, and find a way to assign colours to the edges of the Hamilton cycle.]

14B. Ramsey Theory

Although Ramsey Theory is an important part of Combinatorics (along with Enumeration, Graph Theory, and Design Theory), this course will touch on it only very lightly. The basic idea is that if a very large object is cut into two pieces (or a small number of pieces), then at least one of the pieces must contain a very nice subset. Here is an illustration.

EXAMPLE 14.20. Suppose each edge of K_6 is coloured either red or blue. Show that either there is a triangle whose edges are all red, or there is a triangle whose edges are all blue. That is, K_6 contains a copy of K_3 that has all of its edges of the same colour. For short, we say that K_6 contains a *monochromatic* triangle.

SOLUTION. Choose some vertex v. Since the 5 edges incident with v are coloured with only two colours, the generalized Pigeonhole Principle implies that three of these edges are the same colour. For definiteness, let us say that three edges vu_1, vu_2, and vu_3 are all red.

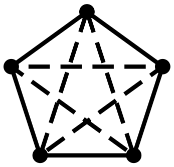
Now, u_1, u_2, and u_3 are the vertices of a copy of K_3 that is inside K_6. If all three edges of this K_3 are blue, then we have our desired monochromatic triangle (namely, a blue triangle). So we may assume that one of the edges is red; say, u_1u_2 is red. Since the edges vu_1 and vu_2 are also red, we see that v, u_1, and u_2 are the vertices of a monochromatic triangle (namely, a red triangle). □

DEFINITION 14.21. Let $k, \ell \in \mathbb{N}^+$.

1) Suppose each edge of K_n is coloured either red or blue. We say **there is a red copy of K_k** if there exist k vertices $u_1, \ldots, u_k$, such that the edge u_iu_j is red for all i and j (with $i \neq j$). Similarly, we say **there is a blue copy of K_ℓ** if there exist ℓ vertices $v_1, \ldots, v_\ell$, such that the edge v_iv_j is blue for all i and j (with $i \neq j$).
2) The **Ramsey number** $R(k, \ell)$ is the smallest number n, such that whenever each edge of K_n is coloured either red or blue, there is always either a red copy of K_k, or a blue copy of K_ℓ.

EXAMPLE 14.22.

1) We have $R(k, 1) = 1$ for all k. This is because K_1 has no edges, so, for any colouring of any K_n, it is true (vacuously) that all of the edges of K_1 are blue.
2) We have $R(k, 2) = k$ for all k. Namely, if some edge is blue, then there is a blue K_2, while if there are no blue edges, then the entire graph is a red K_k.
3) We have $R(3, 3) = 6$. To see this, note that Example 14.20 shows $R(3, 3) \leq 6$, while the edge-colouring of K_5 at right has no monochromatic triangle (because the only monochromatic cycles are of length 5), so $R(3, 3) > 5$.



4) We have $R(k, \ell) = R(\ell, k)$ for all k and ℓ. Namely, if every colouring of K_n has either a red K_k or a blue K_ℓ, then we see that every colouring of K_n must have either a red K_ℓ or a blue K_k, just by switching red and blue in the colouring.

5) If $k \leq k'$ and $\ell \leq \ell'$, then $R(k,\ell) \leq R(k',\ell')$. Namely, we have a colouring of K_n that contains either a red $K_{k'}$ or a blue $K_{\ell'}$. Since $k \leq k'$ and $\ell \leq \ell'$, we know that any $K_{k'}$ contains a copy of K_k, and any $K_{\ell'}$ contains a copy of K_ℓ.

It is not at all obvious that $R(k,\ell)$ exists: theoretically, $R(4,4)$ might not exist, because it might be possible to colour the edges of a very large K_n in such a way that there is no monochromatic K_4. Fortunately, the following extension of the proof of Example 14.20 implies that $R(k,\ell)$ does exist for all k and ℓ. In fact, it provides a bound on how large $R(k,\ell)$ can be (see Exercise 14.24(3) below).

PROPOSITION 14.23. *$R(k,\ell) \leq R(k-1,\ell) + R(k,\ell-1)$ for all $k,\ell \geq 2$.*

PROOF. Let $n = R(k-1,\ell) + R(k,\ell-1)$, and suppose each edge of K_n is coloured either red or blue. We wish to show there is either a red K_k or a blue K_ℓ.

Choose some vertex v of K_n. Then the number of edges incident with v is

$$n-1 = R(k-1,\ell) + R(k,\ell-1) - 1 > \big(R(k-1,\ell)-1\big) + \big(R(k,\ell-1)-1\big),$$

so the very generalized Pigeonhole Principle implies that either $R(k-1,\ell)$ of these edges are red, or $R(k,\ell-1)$ of these edges are blue.

For definiteness, let us assume that the edges $vu_1, vu_2, \ldots, vu_r$ are all blue, where $r = R(k,\ell-1)$. Now, $u_1, u_2, \ldots, u_r$ are the vertices of a copy of K_r that is inside K_n. Since $r = R(k,\ell-1)$, we know that this K_r contains either a red K_k or a blue $K_{\ell-1}$.

If it contains a red K_k, then we have the desired red K_k. So we may assume $u_1, \ldots, u_{\ell-1}$ are the vertices of a blue $K_{\ell-1}$. Since the edges $vu_1, vu_2, \ldots, vu_{\ell-1}$ are also blue, we see that $v, u_1, u_2, \ldots, u_{\ell-1}$ are the vertices of the desired blue K_ℓ. □

EXERCISES 14.24.

1) Show $R(3,4) > 6$.

2) Using Proposition 14.23 and the values of $R(k,\ell)$ given in Example 14.22, find the best upper bound you can on $R(k,\ell)$ for $3 \leq k \leq \ell \leq 6$.

3) Show $R(k,\ell) \leq 2^{k+\ell}$ for all k and ℓ.
[*Hint:* Use Proposition 14.23 and induction on $k+\ell$.]

4) It is known that $40 \leq R(3,10) \leq 42$. Using this information, what can you say about $R(3,11)$?

5) Show there are at least *two* monochromatic triangles in every colouring of the edges of K_6 with two colours.
[*Hint:* Show that there must either be two red (say) triangles, or a red triangle and a blue edge whose endvertices are not in the triangle. Then show that any colouring of the edges joining the red triangle with the blue edge creates either a blue triangle or a second red triangle.]

Remark 14.25. The exact value of $R(k,\ell)$ seems to be extremely difficult to find, except for very small values of k and ℓ. For example, although it has been proved that $R(4,4) = 18$ and $R(4,5) = 25$, no one has been able to determine the precise value of $R(k,\ell)$ for any situation in which k and ℓ are both at least 5. The legendary combinatorist Paul Erdös (1913–1996) said that it would be hopeless to try to calculate the exact value of $R(6,6)$, even with all of the computer resources and brightest minds in the whole world working on the problem for a year. (We do know that $R(6,6)$ is somewhere between 102 and 165.) For more information about the values that have been calculated, see the *Wikipedia* article on Ramsey's theorem.

EXERCISES 14.26. The edges of K_n can also be coloured with more than two colours.

1) Show every colouring of the edges of K_{17} with 3 colours has a monochromatic triangle.
2) Suppose there is a monochromatic triangle in every colouring of the edges of K_n with c colours. Show that if $N - 1 > (c+1)(n-1)$, then every colouring of the edges of K_N with $c + 1$ colours has a monochromatic triangle.

Similar arguments (combined with induction on the number of colours) establish the following very general result.

THEOREM 14.27. Ramsey's Theorem *Given c colours and fixed sizes $n_1, \ldots, n_c \geq 1$, there is an integer*

$$r = R(n_1, \ldots, n_c)$$

such that for any c-colouring of the edges of K_r, there must be some $i \in \{1, \ldots, c\}$ such that K_r has a subgraph isomorphic to K_{n_i} all of whose edges have been coloured with colour i.

PROOF. We will prove this result by induction on c, the number of colours.

Base cases: When $c = 1$, all edges of K_r are coloured with our single colour, so if we let $r = R(n_1) = n_1$, the whole graph is the K_{n_1} all of whose edges have been coloured with colour 1.

We will also require $c = 2$ to be a base case in our induction. In order to prove this second base case, we perform a second proof by induction, this time on $n_1 + n_2$. To make the proof easier to read, we'll call the two colours in any 2-edge-colouring red and blue, and if all of the edges of a K_i have been coloured with one colour, we'll simply call it a red K_i, or a blue K_i.

Base case for the second induction: We'll actually prove a lot of base cases all at once. Since n_1 and n_2 are the number of vertices of a complete graph, we must have $n_1, n_2 \geq 1$. A K_1 has no edges, so vacuously its edges have whichever colour we desire. Thus if $n_1 = 1$ or $n_2 = 1$, we have $r = R(n_1, n_2) = 1$, since for any 2-edge-colouring of K_1, there is a red K_1 and a blue K_1.

Inductive step for the second induction: We begin with the inductive hypothesis. Let $k \geq 2$ be arbitrary. Assume that for every $k_1, k_2 \geq 1$ such that $k_1 + k_2 = k$, there is some integer $r = R(k_1, k_2)$ such that for any 2-edge-colouring of the edges of K_r, there is a subgraph that is either a red K_{k_1} or a blue K_{k_2}.

Let $n_1, n_2 \geq 1$ such that $n_1 + n_2 = k + 1$. If either $n_1 = 1$ or $n_2 = 1$, then this was one of our base cases and the proof is complete, so we may assume that $n_1, n_2 \geq 2$. Therefore, $n_1 - 1, n_2 - 1 \geq 1$, and $n_1 + n_2 - 1 = k$. Now, by our inductive hypothesis, there is some integer $r_1 = R(n_1, n_2 - 1)$ such that for any 2-edge-colouring of the edges of K_{r_1}, there is a subgraph that is either a red K_{n_1} or a blue $K_{n_2 - 1}$. We can also use our inductive hypothesis to conclude that there is some integer $r_2 = R(n_1 - 1, n_2)$ such that for any 2-edge-colouring of the edges of K_{r_2}, there is a subgraph that is either a red $K_{n_1 - 1}$ or a blue K_{n_2}.

We claim that $R(n_1, n_2) \leq r_1 + r_2$. We will show this by proving that any 2-edge-colouring of the edges of $K_{r_1 + r_2}$ must have a subgraph that is either a red K_{n_1}or a blue K_{n_2}.

Consider a complete graph on $r_1 + r_2$ vertices whose edges have been coloured with red and blue. Choose a vertex v, and divide the remaining vertices into two sets: $u \in V_1$ if the edge uv has been coloured red, and $u \in V_2$ if the edge uv has been coloured blue. Since this graph has

$$r_1 + r_2 = |V_1| + |V_2| + 1$$

vertices, we must have either $|V_1| \geq r_2$, or $|V_2| \geq r_1$.

Suppose first that $|V_1| \geq r_2$. Since $r_2 = R(n_1 - 1, n_2)$, the subgraph whose vertices are the elements of V_1 has a subgraph that is either a red $K_{n_1 - 1}$ or a blue K_{n_2}. In the latter case, this subgraph is also in our original $K_{r_1 + r_2}$ and we are done. In the former case, the subgraph whose vertices are the elements of $V_1 \cup \{v\}$ has a red K_{n_1} and we are done.

Suppose now that $|V_2| \geq r_1$ (the proof is similar). Since $r_1 = R(n_1, n_2 - 1)$, the subgraph whose vertices are the elements of V_2 has a subgraph that is either a red K_{n_1} or a blue K_{n_2-1}. In the former case, this subgraph is also in our original $K_{r_1+r_2}$ and we are done. In the latter case, the subgraph whose vertices are the elements of $V_2 \cup \{v\}$ has a blue K_{n_2} and we are done.

By the Principle of Mathematical Induction, for every $n_1, n_2 \geq 1$, there is some integer $r = R(n_1, n_2)$ such that for any colouring of the edges of K_r, there is a subgraph that is either a red K_{n_1} or a blue K_{n_2}.

This second proof by induction completes the proof of the second base case for our original induction on c, the number of colours. We are now ready for the inductive step for our original proof by induction.

Inductive step: We begin with the inductive hypothesis. Let $m \geq 2$ be arbitrary. Assume that for every $k_1, \ldots, k_m \geq 1$, there is an integer $r = R(k_1, \ldots, k_m)$ such that for any m-colouring of the edges of K_r, there must be some $i \in \{1, \ldots, m\}$ such that K_r has a subgraph isomorphic to K_{k_i}, all of whose edges have been coloured with colour i.

Let $n_1, \ldots, n_{m+1}$ be arbitrary. Take a complete graph on

$$r = R(n_1, \ldots, n_{m-1}, R(n_m, n_{m+1}))$$

vertices, and colour its edges with $m + 1$ colours. Temporarily consider the colours m and $m + 1$ to be the same, resulting in a colouring of the edges with m colours. By our inductive hypothesis, there must either be some $i \in \{1, \ldots, m - 1\}$ such that our K_r has a subgraph isomorphic to K_{n_i}, all of whose edges have been coloured with colour i, or K_r has a subgraph isomorphic to $K_{R(n_m,n_{m+1})}$ all of whose edges have been coloured with the mth colour (where this mth colour is really the combination of the colours m and $m + 1$).

If there is some $i \in \{1, \ldots, m - 1\}$ such that our K_r has a subgraph isomorphic to K_{n_i}, all of whose edges have been coloured with colour i, then we are done. The possibility remains that our K_r has a subgraph isomorphic to $K_{R(n_m,n_{m+1})}$ all of whose edges have been coloured with either colour m or colour $m + 1$. But by our base case for $c = 2$, this graph must have either a subgraph isomorphic to K_{n_m} all of whose edges have been coloured with colour m, or a subgraph isomorphic to $K_{n_{m+1}}$ all of whose edges have been coloured with colour $m + 1$. This completes the inductive step.

By the Principle of Mathematical Induction, for every $c \geq 1$ and fixed sizes $n_1, \ldots, n_c \geq 1$, there is an integer $r = R(n_1, \ldots, n_c)$ such that for any c-colouring of the edges of K_r, there must be some $i \in \{1, \ldots, c\}$ such that K_r has a subgraph isomorphic to K_{n_i} all of whose edges have been coloured with colour i. □

EXERCISES 14.28.

1) Find $R(2, 2, 3)$.

2) Find $R(2, 4)$.

3) Find a 2-edge-colouring of K_6 that does not have a K_4 of either colour.

EXERCISE 14.29. (Schur's Theorem) Let $c \in \mathbb{N}^+$, and let $N = R(3, \ldots, 3)$ where there are c entries (all equal to 3). If $\{A_1, A_2, \ldots, A_c\}$ is any partition of $\{1, 2, \ldots, N\}$ into c subsets, show that some A_i contains three integers x, y, and z, such that $x + y = z$.
[*Hint:* The vertices of K_N are $1, 2, \ldots, N$. Put colour i on each edge uv with $|u - v| \in A_i$. If u, v, w are the vertices of a monochromatic triangle of colour i, with $u > v > w$, then $\{u - v, v - w, u - w\} \subseteq A_i$, and we have $(u - v) + (v - w) = u - w$.]

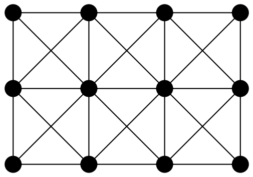
14C. Vertex colouring

Suppose you have been given the task of assigning broadcast frequencies to transmission towers. You have been given a list of frequencies that you are permitted to assign. There is a constraint: towers that are too close together cannot be assigned the same frequency, since they would interfere with each other.

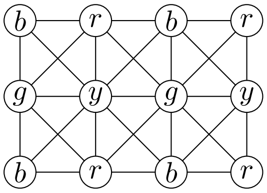
One way to approach this problem is to model it as a graph. The vertices of the graph will represent the towers, and the edges will represent towers that can interfere with each other. Your job is to assign a frequency to each of the vertices. Instead of writing a frequency on each vertex, we will choose a colour to represent that frequency, and use that colour to colour the vertices to which you assign that frequency.

Here is an example of this.

EXAMPLE 14.30. This graph represents the towers and their interference patterns.



This represents a possible assignment of 4 colours to the vertices. The colour of each vertex (red, green, blue, or yellow) is indicated by writing the first letter of the colour's name on the vertex).



Notice that this colouring obeys the constraint that interfering towers are not assigned the same frequencies.

DEFINITION 14.31. A **proper k-vertex-colouring** (or just k-colouring) of a graph G is a function that assigns to each vertex of G one of k colours, such that adjacent vertices must be assigned different colours.

As with edge-colouring, the constraint that adjacent vertices receive different colours turns out to be a useful constraint that arises in many contexts. We often represent the k colours by the numbers $1, \ldots, k$, and label the vertices with the appropriate numbers rather than colouring them.

DEFINITION 14.32. A graph G is **k-colourable** if it admits a proper k-(vertex-)colouring. The smallest integer k for which G is k-colourable is called the **chromatic number** of G.

NOTATION 14.33. The chromatic number of G is denoted by $\chi(G)$, or simply by χ if the context is unambiguous.

We leave the proof of the following as an exercise (see Exercise 14.43(2)).

PROPOSITION 14.34. *For every $n \geq 1$, $\chi(K_n) = n$.*

EXAMPLE 14.35. Prove that for a graph G, $\chi(G) = 2$ if and only if G is a bipartite graph that has at least one edge.

SOLUTION. Proof. **(⇒)** Suppose that $\chi(G) = 2$. Take a proper 2-colouring of G with colours 1 and 2. Let V_1 denote the set of vertices of colour 1, and let V_2 denote the set of vertices of colour 2. Since the colouring is proper, there are no edges both of whose endvertices are in V_1 (as these would be adjacent vertices both coloured with colour 1). Similarly, there are no edges both of whose endvertices are in V_2. Thus, the sets V_1 and V_2 form a bipartition of G, so G is bipartite. Since 2 colours were required to properly colour G, G must have at least one edge.

(⇐) Suppose that G is bipartite, and that V_1 and V_2 form a bipartition of G. Colour the vertices in V_1 with colour 1, and colour the vertices of V_2 with colour 2. By the definition of a bipartition, no pair of adjacent vertices can have been assigned the same colour. Thus, this is a proper 2-colouring of G, so $\chi(G) \leq 2$. Since G has at least one edge, the endpoints of that edge must be assigned different colours, so $\chi(G) \geq 2$. Thus $\chi(G) = 2$. □

EXAMPLE 14.36. Show that for any $n \geq 1$, $\chi(C_{2n+1}) = 3$.

SOLUTION. Since this graph has an edge whose endvertices must be assigned different colours, we see that $\chi(C_{2n+1}) \geq 2$. Since a cycle of odd length is not bipartite (see Theorem 14.13), Example 14.35 shows that $\chi(C_{2n+1}) \neq 2$, so $\chi(C_{2n+1}) \geq 3$. Let the cycle be $(u_1, u_2, \ldots, u_{2n+1}, u_1)$. Since the only edges in the graph are between consecutive vertices in this list, if we assign colour 1 to u_1, colour 2 to u_{2i} for $1 \leq i \leq n$, and colour 3 to u_{2i+1} for $1 \leq i \leq n$, this will be a proper 3-colouring. Thus, $\chi(C_{2n+1}) = 3$. □

DEFINITION 14.37. A graph G is ***k*-critical** if $\chi(G) = k$, but for every proper subgraph H of G, $\chi(H) < \chi(G)$.

PROPOSITION 14.38. *Any k-critical graph is connected.*

PROOF. Towards a contradiction, suppose that G is a disconnected k-critical graph, and let G_1 and G_2 be (nonempty) subgraphs of G such that every vertex of G is in either G_1 or G_2, and there is no edge from any vertex in G_1 to any vertex in G_2. By the definition of k-critical, $\chi(G_1) < \chi(G)$ and $\chi(G_2) < \chi(G)$. But if we colour G_1 with $\chi(G_1)$ colours and G_2 with $\chi(G_2)$ colours, since there is no edge from any vertex of G_1 to any vertex of G_2, this produces a proper colouring of G with

$$\max(\chi(G_1), \chi(G_2)) < \chi(G)$$

colours. This contradiction serves to prove that every k-critical graph is connected. □

THEOREM 14.39. *If G is k-critical, then $\delta(G) \geq k - 1$.*

PROOF. Towards a contradiction, suppose that G is k-critical and has a vertex v of valency at most $k-2$. By the definition of k-critical, $G \setminus \{v\}$ must be $(k-1)$-colourable. Now, since v has no more than $k-2$ neighbours, its neighbours can be assigned at most $k-2$ distinct colours in this colouring. Therefore, amongst the colours used in the $(k-1)$-colouring of $G \setminus \{v\}$, there must be a colour that is not assigned to any of the neighbours of v. If we assign this colour to v, the result is a proper $(k-1)$-colouring of G, contradicting $\chi(G) = k$. This contradiction serves to prove that every k-critical graph has minimum valency at least $k-1$. □

COROLLARY 14.40. *For any graph G, $\chi(G) \leq \Delta(G) + 1$.*

PROOF. Let G be an arbitrary graph. By deleting as many edges and vertices as it is possible to delete without reducing the chromatic number (we can never increase the chromatic number by deleting vertices or edges, see Exercise 14.43(1)), we see that G must have a subgraph H that is $\chi(G)$-critical. By Theorem 14.39, we see that

$$\delta(H) \geq \chi(G) - 1.$$

Thus, every vertex of H has valency at least $\chi(G) - 1$, so in G, these same vertices still have valency at least $\chi(G) - 1$. For any such vertex v, we have

$$\Delta(G) \geq d(v) \geq \chi(G) - 1,$$

so $\chi(G) \leq \Delta(G) + 1$. □

We have already seen two families of graphs for which this bound is attained: for complete graphs, we have

$$\Delta(K_n) + 1 = (n-1) + 1 = n = \chi(K_n)$$

(see Proposition 14.34); and for cycles of odd length, we have

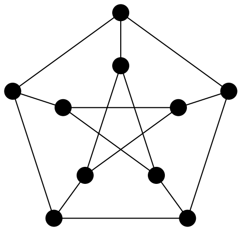
$$\Delta(C_{2n+1}) + 1 = 2 + 1 = 3 = \chi(C_{2n+1})$$

(see Example 14.36). In fact, Brooks proved in 1941 that these are the only connected graphs for which this bound is obtained.

THEOREM 14.41. Brooks' Theorem *If G is connected and for every $n \geq 1$, $G \ncong C_{2n+1}$ and $G \ncong K_n$, then $\chi(G) \leq \Delta(G)$.*

We will not include the proof of this result in this course. This theorem does allow us to determine the chromatic number of some graphs with very little work.

EXAMPLE 14.42. The following very famous graph is called the **Petersen graph**. It is an exceptional graph in many ways, so when mathematicians are trying to come up with a proof or a counterexample in graph theory, it is often one of the first examples they will check. Find its chromatic number.



SOLUTION. We have $\Delta = 3$, and since this graph is neither a complete graph nor a cycle of odd length, by Brooks' Theorem this shows that $\chi \leq 3$. We can find a cycle of length 5 around the outer edge of the graph, so this graph is not bipartite but has an edge. Therefore (by Example 14.35), $\chi > 2$. Hence $\chi = 3$. □

EXERCISES 14.43.

1) Prove that if H is a subgraph of G then $\chi(G) \geq \chi(H)$.

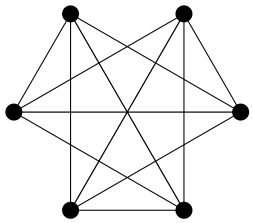
2) Prove Proposition 14.34 by induction.

3) Prove Corollary 14.40 by induction for every graph on at least one vertex.

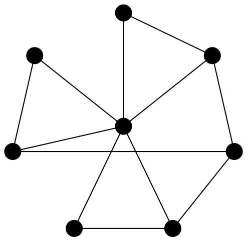
4) For each $i, j \in \{4, 5, 6\}$, suppose you are given a graph G that contains a subgraph isomorphic to K_i and no vertex has more than j neighbours. What (if anything) can you say about $\chi(G)$? Can you say more if you know that G is connected and is neither a complete graph nor a cycle of odd length?

EXERCISES 14.44. For each of the following graphs, determine its chromatic number by using theoretical arguments to provide a lower bound, and then producing a colouring that meets the bound. Do the same for the edge-chromatic number.

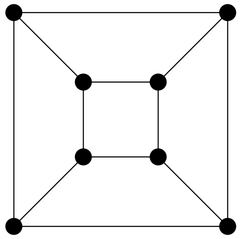
1)



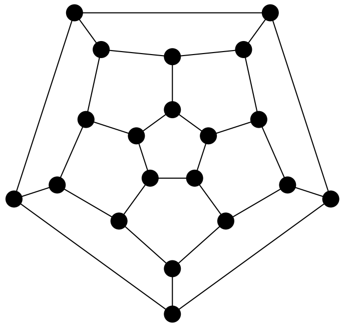
2)



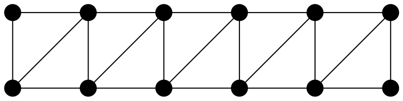
3)



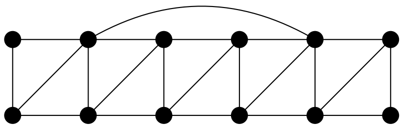
4)



5)



6)



SUMMARY:

- Vizing's Theorem
- graphs are bipartite if and only if they contain no cycle of odd length
- Ramsey's Theorem
- graphs are bipartite if and only if they are 2-colourable
- Brooks' Theorem
- Petersen graph
- Important definitions:
  - proper k-edge-colouring, k-edge-colourable
  - edge chromatic number, chromatic index
  - class one graph, class two graph
  - bipartite, bipartition
  - complete bipartite graph
  - proper k-colouring, k-colourable
  - chromatic number
  - k-critical
- Notation:
  - $\chi'(G)$
  - $K_{m,n}$
  - $R(n_1, \ldots, n_c)$
  - $\chi(G)$

Chapter 15

Planar graphs

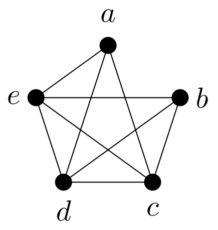
15A. Planar graphs

Visually, there is always a risk of confusion when a graph is drawn in such a way that some of its edges cross over each other. Also, in physical realisations of a network, such a configuration can lead to extra costs (think about building an overpass as compared with building an intersection). It is therefore helpful to be able to work out whether or not a particular graph can be drawn in such a way that no edges cross.

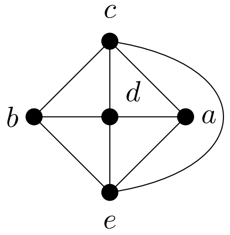
DEFINITION 15.1. A graph is **planar** if it can be drawn in the plane ($\mathbb{R}^2$) so edges that do not share an endvertex have no points in common, and edges that do share an endvertex have no other points in common.

Such a drawing is called a **planar embedding** of the graph.

EXAMPLE 15.2. The following graph is planar:



Here is a planar embedding:



THEOREM 15.3. *The graph K_5 is not planar.*

PROOF. Label the vertices of K_5 as $v_1, \ldots, v_5$. Consider the 3-cycle (v_1, v_2, v_3, v_1). The vertex v_4 must lie either inside or outside the boundary determined by this 3-cycle. Furthermore, since there is an edge between v_4 and v_5, the vertex v_5 must lie on the same side (inside or outside) as v_4.

Suppose first that v_4 and v_5 lie inside the boundary. The edges v_1v_4, v_2v_4, and v_3v_4 divide the area inside the boundary into three regions, and v_5 must lie inside one of these three regions.

One of v_1, v_2, and v_3 is not a corner of this region, and in fact lies outside of it while v_5 lies inside of it, making it impossible to draw the edge from this vertex to v_5.

The proof is similar if v_4 and v_5 lie on the outside of the boundary determined by the 3-cycle (v_1, v_2, v_3, v_1). □

THEOREM 15.4. *The complete bipartite graph $K_{3,3}$ is not planar.*

PROOF. Label the vertices in one of the bipartition sets as v_1, v_2, v_3, and the vertices in the other part as u_1, u_2, u_3. Consider the 4-cycle

$$(v_1, u_1, v_2, u_2, v_1).$$

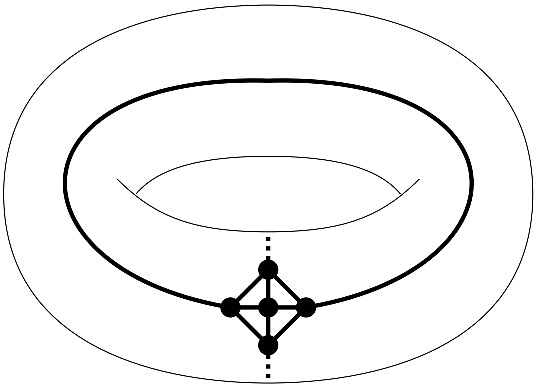
The vertex v_3 must lie either inside or outside the boundary determined by this 4-cycle. Furthermore, since there is an edge between v_3 and u_3, the vertex u_3 must lie on the same side (inside or outside) as v_3.

Suppose first that v_3 and u_3 lie inside the boundary. The edges v_3u_1 and v_3u_2 divide the area inside the boundary into two regions, and u_3 must lie inside one of these two regions. One of v_1 and v_2 does not lie on the boundary of this region, and in fact lies outside of it while u_3 lies inside of it, making it impossible to draw the edge from this vertex to u_3.

The proof is similar if v_3 and u_3 lie on the outside of the boundary determined by the 4-cycle $(v_1, u_1, v_2, u_2, v_1)$. □

However, both K_5 and $K_{3,3}$ can be embedded onto the surface of what we call a torus (a doughnut shape), with no edges meeting except at mutual endvertices. Embeddings are shown in Figures 15.1 and 15.2.

Figure 15.1. K_5 embedded on a torus



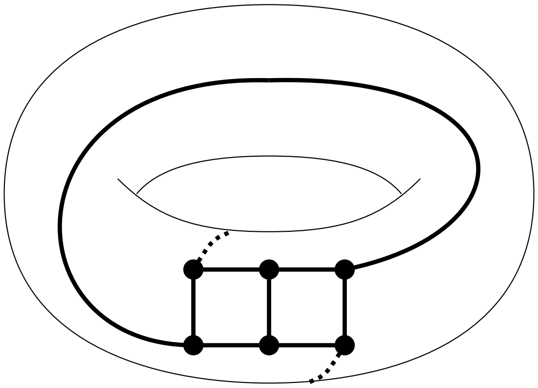
The dotted edge wraps around through the hole in the torus.

You might think at this point that every graph can be embedded on the torus without edges meeting except at mutual endvertices, but this is not the case. In fact, for any surface there are graphs that cannot be embedded in that surface (without any edges meeting except at mutual endvertices).

For any embedding of a planar graph, there is another embedded planar graph that is closely related to it, which we will now describe. Notice that a planar embedding partitions the plane into regions.

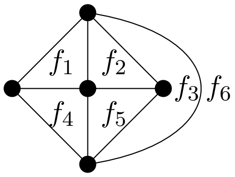
DEFINITION 15.5. The regions into which a planar embedding partitions the plane, are called the **faces** of the planar embedding.

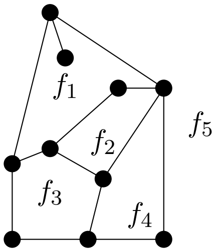
Figure 15.2. $K_{3,3}$ embedded on a torus



The dotted edge wraps around through the hole in the torus.

EXAMPLE 15.6. In these drawings, we have labeled the faces of the two planar embeddings with f_1, f_2, etc., to show them clearly.





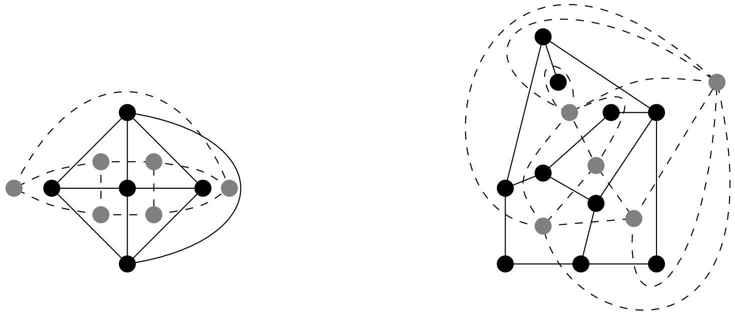
NOTATION 15.7. We use $F(G)$ (or simply F if the graph is clear from the context) to denote the set of faces of a planar embedding.

DEFINITION 15.8. We say that an edge is **incident with a face** of a planar embedding, if it lies on the boundary of the face (or inside the face).

For a planar embedding of G, the **dual graph** or **planar dual**, G^*, is defined by $V(G^*) = F(G)$, and $f_i \sim f_j$ if and only if there is an edge of G that is incident with both f_i and f_j.

It is possible that the dual graph of a planar embedding will not be a simple graph, even if the original graph was simple.

EXAMPLE 15.9. Here we show how to find the planar duals of the embeddings given in Example 15.6. We include the original embedding as above; the grey vertices and dashed edges are the vertices and edges of the dual graph.



Note that the second graph has loops and multiedges. Note also that although f_1 and f_5 meet at a vertex in the embedding of the first graph, they are not adjacent in the dual since they do not share a common edge.

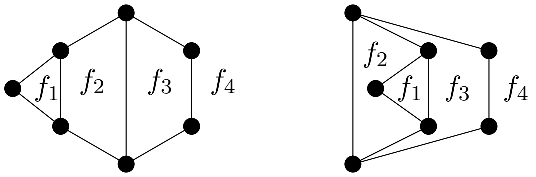
Some other useful observations:

- $|E(G)| = |E(G^*)|$, and every dashed edge crosses exactly one black edge;
- the valency of the vertex f_i in G^* is equal to the number of edges you trace, if you trace around the perimeter of the face f_i in G (so edges that dangle inside the face get counted twice).

PROPOSITION 15.10. *The dual graph of a planar embedding has a natural planar embedding, so is a planar graph. Furthermore,* $(G^*)^* = G$.

Both of these facts follow fairly directly from the definitions.

EXAMPLE 15.11. Be careful! – Two different planar embeddings of the same graph may have nonisomorphic dual graphs, as we show here.



In the planar dual of the embedding on the left, f_1 will have valency 3; f_2 and f_3 will have valency 4; and f_4 will have valency 7. In the planar dual of the embedding on the right, f_1 will have valency 3; f_2 will have valency 5; f_4 will have valency 4, and f_3 will have valency 6. Since the lists $3, 4, 4, 7$ and $3, 4, 5, 6$ are not permutations of each other, the planar duals cannot be isomorphic.

Before moving on to other related topics, we present a classification of planar graphs. This is a theorem by Kuratowski (from whose name the notation for complete graphs is taken). He proved this result in 1930.

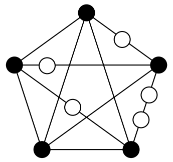
We need one new definition.

DEFINITION 15.12. An edge uv can be **subdivided** by placing a vertex somewhere along its length. Technically, this means deleting uv, adding a new vertex x, and adding the edges ux and vx.

A **subdivision** of a graph is a graph that is obtained by subdividing some of the edges of the graph.

EXAMPLE 15.13. An example is shown in Figure 15.3. The white vertices are the new ones.

Figure 15.3. A subdivision of K_5



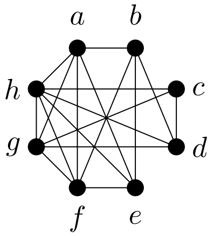
THEOREM 15.14. Kuratowski's Theorem *A graph G is planar if and only if no subgraph of G is a subdivision of K_5 or $K_{3,3}$.*

One direction of the proof is fairly straightforward, since we have already proven that K_5 and $K_{3,3}$ are not planar. However, we won't try to prove this theorem in this course.

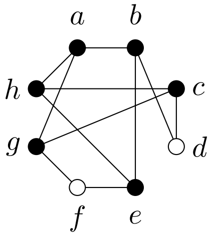
A subdivision of K_5 or of $K_{3,3}$ will sometimes be very difficult to find, but efficient algorithms do exist.

Typically, to prove that a graph is planar you would find a planar embedding. To prove that a graph is not planar, you would find a subgraph that is a subdivision of either K_5 or $K_{3,3}$.

EXAMPLE 15.15. Find a subgraph that is a subdivision of K_5 or $K_{3,3}$ in this graph, to show that it is not planar.



SOLUTION. Here is a subdivision of $K_{3,3}$ in the given graph. The white vertices are the vertices that are subdividing edges. Unnecessary edges have been deleted. The bipartition consists of $\{a, c, e\}$ and $\{b, g, h\}$.

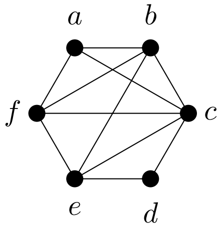


□

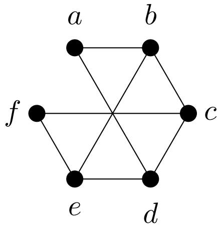
EXERCISES 15.16.

1) Prove that if a graph G has a subgraph H that is not planar, then G is not planar. Deduce that for every $n \geq 6$, K_n is not planar.

2) Find a planar embedding of the following graph, and find the dual graph of your embedding:



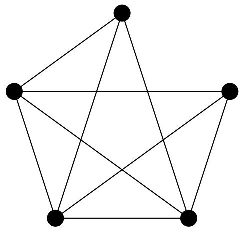
3) Find a planar embedding of the following graph, and find the dual graph of your embedding:

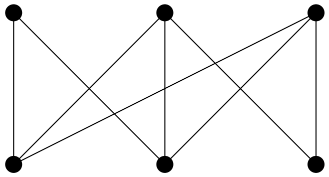


4) The graph in Example 15.15 also has a subgraph that is a subdivision of K_5. Find such a subgraph.

5) Prove that the Petersen graph is not planar.
[*Hint:* Use Kuratowski's Theorem.]

6) Find planar embeddings of the two graphs pictured below. (These graphs are obtained by deleting an edge from K_5 and deleting an edge from $K_{3,3}$, respectively.)





15B. Euler's Formula

Euler came up with a formula that holds true for any planar embedding of a connected graph.

THEOREM 15.17. Euler's Formula *If G is a planar embedding of a connected graph (or multigraph, with or without loops), then*

$$|V| - |E| + |F| = 2.$$

PROOF 1. We will prove this formula by induction on the number of faces of the embedding. Let G be a planar embedding of a connected graph (or multigraph, with or without loops).

Base case: If $|F| = 1$ then G cannot have any cycles (otherwise the interior and exterior of the cycle would be 2 distinct faces). So G must be a connected graph that has no cycles, i.e., a tree. By Theorem 12.27 we know that we must have $|E| = |V| - 1$, so

$$|V| - |E| + |F| = |V| - (|V| - 1) + 1 = 2.$$

A tree cannot have any loops or multiple edges, as these form cycles.

Inductive step: We begin by stating our inductive hypothesis. Let $k \geq 1$ be arbitrary, and assume that for any planar embedding of a connected graph (or multigraph, with or without loops) with k faces, $|V| - |E| + |F| = 2$.

Let G be a planar embedding of a connected graph with $k+1 \geq 2$ faces. Since trees have only one face, G must have a cycle. Choose any edge e that is in a cycle of G, and let $H = G \setminus \{e\}$. Clearly, we have

$$|E(H)| = |E(G)| - 1$$

and $|V(H)| = |V(G)|$. Also,

$$|F(H)| = |F(G)| - 1 = k$$

since the edge e being part of a cycle must separate two faces of G, which are united into one face of H. Furthermore, since e was in a cycle and G is connected, by Proposition 12.21 H is connected, and H has a planar embedding induced by the planar embedding of G. Therefore our inductive hypothesis applies to H, so

$$\begin{aligned} 2 &= |V(H)| - |E(H)| + |F(H)| \\ &= |V(G)| - (|E(G) - 1) + (|F(G)| - 1) \\ &= |V(G)| - |E(G)| + |F(G)| \end{aligned}$$

This completes the inductive step.

By the Principle of Mathematical Induction, $|V| - |E| + |F| = 2$ for any planar embedding of a connected graph (or multigraph, with or without loops). □

The above proof is unusual for a proof by induction on graphs, because the induction is not on the number of vertices. If you try to prove Euler's formula by induction on the number of vertices, deleting a vertex might disconnect the graph, which would mean the induction hypothesis doesn't apply to the resulting graph.

However, there is a different graph operation that reduces the number of vertices by 1, and keeps the graph connected. Unfortunately, it may turn a graph into a multigraph, so it can only be used to prove a result that holds true for multigraphs as well as for graphs. This operation is called *edge contraction*.

DEFINITION 15.18. Let G be a graph with an edge uv. The graph G' obtained by **contracting the edge uv** has vertices

$$V(G') = (V(G) \setminus \{u, v\}) \cup \{u'\},$$

where u' is a new vertex. The edges are

$$E(G') = \big([E(G) \setminus \{ux : ux \in E(G)\}] \setminus \{vx : vx \in E(G)\}\big) \cup \{u'y \mid uy \in E(G) \text{ or } vy \in E(G)\}.$$

If you think of vertices u and v as being connected by a very short elastic that has been stretched out in G, then you can think of G' as the graph you get if you allow the elastic to contract, combining the vertices u and v into a "new" vertex u'.

Notice that if G is connected, then the graph obtained by contracting any edge of G will also be connected. However, if uv is the edge that we contract, and u and v have a mutual neighbour x, then in the graph obtained by contracting uv, there will be a multiple edge between u' and x. Also, if G has a planar embedding, then after contracting any edge there will still be a planar embedding. If $u \neq v$, then contracting uv reduces the number of vertices by one, reduces the number of edges by one, and does not change the number of faces.

Now we can use this operation to prove Euler's formula by induction on the number of vertices.

PROOF 2. Let G be a planar embedding of a connected graph (or multigraph, with or without loops).

Base case: If $|V| = 1$ then G has one vertex. Furthermore, every edge is a loop. Every loop involves 1 edge, and encloses 1 face. This graph will therefore have one more face than it has loops (since it has one face even if there are no loops). Thus,

$$|V| - |E| + |F| = 1 - e + (e+1) = 2.$$

Inductive step: We begin by stating our inductive hypothesis. Let $k \geq 1$ be arbitrary, and assume that for any planar embedding of a connected graph (or multigraph, with or without loops) with k vertices, $|V| - |E| + |F| = 2$.

Let G be a planar embedding of a connected graph with $k+1 \geq 2$ vertices. Since the graph is connected and has at least two vertices, it has at least one edge uv, with $u \neq v$. Let G' be the graph we obtain by contracting uv. Then G' is a planar embedding of a connected graph (or multigraph, with or without loops) on k vertices, so our inductive hypothesis applies to G'. Therefore,

$$\begin{aligned} 2 &= |V(G')| - |E(G')| + |F(G')| \\ &= (|V(G)| - 1) - (|E(G) - 1) + |F(G)| \\ &= |V(G)| - |E(G) + |F(G)| \end{aligned}$$

This completes the inductive step.

By the Principle of Mathematical Induction, $|V| - |E| + |F| = 2$ for any planar embedding of a connected graph (or multigraph, with or without loops). □

Contraction of edges has some other very important uses in graph theory. Before looking at some corollaries of Euler's Formula, we'll explain one well-known theorem that involves edge contraction and planar graphs.

DEFINITION 15.19. Let G be a graph. Then H is a **minor** of G if we can construct H from G by deleting or contracting edges, and deleting vertices.

In 1937, Wagner proved a theorem quite similar to Kuratowski's.

THEOREM 15.20. Wagner's Theorem *A graph is planar if and only if it has no minor isomorphic to K_5 or $K_{3,3}$.*

It is possible to prove Wagner's Theorem as an easy consequence of Kuratowski's Theorem, since if G has a subgraph that is a subdivision of K_5 or $K_{3,3}$ then contracting all but one piece of each subdivided edge gives us a minor that is isomorphic to K_5 or $K_{3,3}$. Nonetheless, Wagner's Theorem is important in its own right, as the first example of the much more recent and very powerful work by Neil Robertson and Paul Seymour on graph minors.

A family is said to be *minor-closed* if given any graph in the family, any minor of the graph is also in the family. Planar graphs are an example of a minor-closed family, since the operations of deletion (of edges or vertices) and contraction of edges preserve a planar embedding. Robertson and Seymour proved the remarkable result that if a family of graphs is minor-closed, then the family can be characterised by a *finite* set of "forbidden minors." That is, for any such family $\mathcal{F}$, there is a finite set $\mathcal{L}$ of graphs, such that $G \in \mathcal{F}$ if and only if no minor of G appears in $\mathcal{L}$. Wagner's Theorem tells us that when $\mathcal{F}$ is the family of planar graphs, $\mathcal{L} = \{K_5, K_{3,3}\}$.

Euler's Formula has some important corollaries.

COROLLARY 15.21. *Let G be a connected graph. Then every planar embedding of G has the same number of faces.*

PROOF. We have $|V| - |E| + |F| = 2$. Since $|V|$ and $|E|$ do not depend on the choice of embedding, we have $|F| = 2 + |E| - |V|$ cannot depend on the choice of embedding. □

COROLLARY 15.22. *If G is a simple connected planar graph and $|V| \geq 3$, then*

$$|E| \leq 3|V| - 6.$$

If in addition, G has no cycles of length less than 4, then $|E| \leq 2|V| - 4$.

COMBINATORIAL PROOF. Fix a planar embedding of G. We move around each face, counting the number of edges that we encounter, and work out the result in two ways.

First, we look at every face in turn and count how many edges surround that face. Since the graph is simple, every face must be surrounded by at least 3 edges unless there is only one face. If there is only one face and when moving around this face we do not count at least 3 edges, then the graph is a tree that has at most one edge, so $|V| \leq 2$. Therefore, our count will come to at least $3|F|$.

Every edge either separates two faces, or dangles into a face. In the former case, it will be counted once each time we move around one of the two incident faces. In the latter case, it will be counted twice as we move around the face it dangles into: once when we move inwards along this dangling part, and once when we move back outward. Thus, every edge is counted exactly twice, so our count will come to exactly $2|E|$.

Combining these, we see that $2|E| \geq 3|F|$, so $|F| \leq 2|E|/3$. If G has no cycles of length less than 4, then every face must be surrounded by at least 4 edges, so the same argument gives $2|E| \geq 4|F|$, so $|F| \leq |E|/2$.

By Euler's Formula, $|V| - |E| + |F| = 2$, so

$$|V| - |E| + 2|E|/3 \geq 2.$$

Multiplying through by 3 and moving the $|E|$ terms to the right-hand side, gives

$$3|V| \geq |E| + 6,$$

which can easily be rearranged into the form of our original statement. In the case where G has no cycles of length less than 4, we obtain instead

$$|V| - |E| + |E|/2 \geq 2,$$

so $2|V| \geq |E| + 4$, which again can easily be rearranged into the form given in the statement of this corollary. □

COROLLARY 15.23. *If G is a simple connected planar graph, then $\delta(G) \leq 5$.*

PROOF. Towards a contradiction, suppose that G is a simple connected planar graph, and for every $v \in V$, $d(v) \geq 6$. Then

$$\sum_{v \in V} d(v) \geq 6|V|.$$

By Euler's handshaking lemma, this gives

$$\sum_{v \in V} d(v) = 2|E| \geq 6|V|.$$

Therefore,

$$|E| \geq 3|V| > 3|V| - 6,$$

but this contradicts Corollary 15.22. □

Euler's Formula (and its corollaries) give us a much easier way to prove that K_5 and $K_{3,3}$ are non-planar.

COROLLARY 15.24. *The graph K_5 is not planar.*

PROOF. In K_5 we have $|E| = \binom{5}{2} = 10$, and $|V| = 5$. So

$$3|V| - 6 = 15 - 6 = 9 < 10 = |E|.$$

By Corollary 15.22, K_5 must not be planar. □

COROLLARY 15.25. *The graph $K_{3,3}$ is not planar.*

PROOF. In $K_{3,3}$ we have $|E| = 9$, and $|V| = 6$. So

$$2|V| - 4 = 12 - 4 = 8 < 9 = |E|.$$

Since $K_{3,3}$ is bipartite, it has no cycles of length less than 4, so by Corollary 15.22, $K_{3,3}$ must not be planar. □

EXERCISES 15.26.

1) Use induction to prove an Euler-like formula for planar graphs that have exactly two connected components.

2) Euler's formula can be generalised to disconnected graphs, but has an extra variable for the number of connected components of the graph. Guess what this formula will be, and use induction to prove your answer.

3) Find and prove a corollary to Euler's formula for disconnected graphs, similar to Corollary 15.22. (Use your answer to question 2.)

4) For graphs embedded on a torus, $|V| - |E| + |F|$ has a different (but constant) value, as long as all of the faces "look like" discs. (If you are familiar with topology, the faces must be embeddable into a plane, rather than looking like a torus. So putting a planar embedding of a graph down on one side of a torus doesn't count.) What is this value?

5) **Definition.** We say that a planar embedding of a graph is *self-dual* if it is isomorphic to its planar dual.

   Prove that if a planar embedding of the connected graph G is self-dual, then $|E| = 2|V| - 2$.

6) **Definition.** The *complement* of G is the graph with the same vertices as G, but whose edges are precisely the *non*-edges of G. (That is, u is adjacent to v in the complement of G if and only u is *not* adjacent to v in G.) Therefore, if G^c is the complement of G, then $E(K_{|V(G)|})$ is the disjoint union of $E(G)$ and $E(G^c)$.

   Show that if G is a simple planar graph with at least eleven vertices, then the complement of G is not planar.

7) Find a planar graph G with $|V| = 8$ whose complement is also planar.

8) For each of the following sets of conditions, either draw a connected, simple graph G in the plane that satisfies the conditions, or explain how you know that there isn't one.

   (a) The graph has 15 vertices and 12 edges.

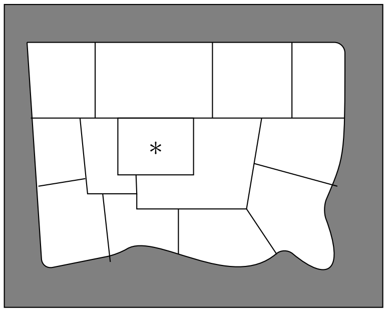
   (b) The graph has 10 vertices and 33 edges.

   (c) The graph has 5 vertices and 8 edges.

   (d) The graph has 6 vertices and 9 edges, and the embedding has 6 faces.

15C. Map colouring

Suppose we have a map of an island that has been divided into states.



Traditionally, map-makers colour the different states so as to ensure that if two states share a border, they are not coloured with the same colour. (This makes it easier to distinguish the borders.) If two states simply meet at a corner, then they may be coloured with the same colour.

Using additional colours used to add to the cost of producing the map. Also, if there are too many colours they become harder and harder to distinguish amongst. The question is, without knowing in advance what the map will look like, is there a bound on how many colours will be required to colour it? If so, what is that bound? In other words, what is the largest number of colours that might be required to colour some map?

Well over a century ago, mathematicians observed that it never seemed to require more than 4 colours to colour a map. The map shown above does require 4 colours, since the central rectangular state (marked with an asterisk) and the three states that surround it must all receive different colours (each shares a border with each of the others). Unfortunately, they couldn't prove that no more would ever be required, although a number of purported proofs were published and later found to have errors.

Although the bound of 4 eluded many attempts at proof, in 1890 Percy John Heawood successfully proved that 5 colours suffice to colour any map. (His method was based on an incorrect proof of the Four Colour Theorem by Kempe, from 1879.) This result is known as the Five Colour Theorem. Its proof is slightly technical but not difficult, and we will give it in a moment. First we will give a very short proof that 6 colours suffice.

Notice that if we turn the map into a graph by placing a vertex wherever borders meet, and an edge wherever there is a border, this problem is equivalent to finding a proper vertex colouring of the planar dual of this graph. Thus, what we will actually prove is that the vertices of any planar graph can be properly coloured using 6 (or in the subsequent result, 5) colours. There is a detail that we are skimming over here: the planar dual could have loops, which would make it impossible to colour the graph. However, this can only happen if there is a face of the original map that meets itself along a border, which would never happen in a map. The planar dual might also have multiedges, but this does not affect the number of colours required to properly colour the graph, so we can delete any multiedges and assume that we are dealing with a simple planar graph.

PROPOSITION 15.27. *Every planar graph is properly 6-colourable.*

PROOF. Towards a contradiction, suppose that there is a planar graph that is not properly 6-colourable. By deleting edges and vertices, we can find a subgraph G that is a 7-critical planar graph.

By Corollary 15.23, we must have $\delta(G) \leq 5$ since G is planar. But by Theorem 14.39, we must have

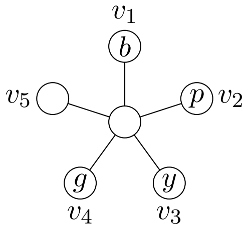
$$\delta(G) \geq 7 - 1 = 6$$

since G is 7-critical. This contradiction serves to prove that every planar graph is properly 6-colourable. □

THEOREM 15.28. Five Colour Theorem *Every planar graph is properly 5-colourable.*

PROOF. Towards a contradiction, suppose that there is a planar graph that is not properly 5-colourable. By deleting edges and vertices, we can find a subgraph G that is a 6-critical planar graph. Since G is planar, Corollary 15.23 tells us that $\delta(G) \leq 5$. We also know from Theorem 14.39 that $\delta(G) \geq 6-1 = 5$ since G is 6-critical. Let v be a vertex of valency $\delta(G) = 5$.

By the definition of a k-critical graph, $G \setminus \{v\}$ can be properly 5-coloured. Since G itself cannot be properly 5-coloured, the neighbours of v must all have been assigned different colours in the proper 5-colouring of $G \setminus \{v\}$. Let's label the neighbours of v as v_1, v_2, v_3, v_4, and v_5 as they appear clockwise around v. We will call the colour of v_1 blue, the colour of v_2 purple, the colour of v_3 yellow, and the colour of v_4 green, as shown in the picture. Here is a picture (where, because this text is printed in black-and-white, we have put the first letter of a colour onto a vertex, instead of actually colouring the vertex).



Consider the subgraph consisting of the vertices coloured blue or yellow (and all edges between such vertices). If v_1 and v_3 are not in the same connected component of this subgraph, then in the connected component that contains v_1, we could interchange the colours yellow and blue. Since we are doing this to everything in a connected component of the yellow-blue subgraph, the result will still be a proper colouring, but v_1 now has colour yellow, so v can be coloured with blue. This contradicts the fact that G is 6-critical, so it must be the case that v_1 and v_3 are in the same connected component of the yellow-blue subgraph. In particular, there is a walk from v_1 to v_3 that uses only yellow and blue vertices. By Proposition 12.16, there is in fact a path from v_1 to v_3 that uses only yellow and blue vertices.

Similarly, if we consider the subgraph consisting of the vertices coloured purple or green (and all edges between such vertices), we see that there must be a path from v_2 to v_4 that uses only purple or green vertices.

There is no way to draw the yellow-blue path from v_1 to v_3 and the purple-green path from v_2 to v_4, without the two paths crossing each other. Since the graph is planar, they must cross each other at a vertex, u. Since u is on the yellow-blue path, it must be coloured either yellow or blue. Since u is on the purple-green path, it must be coloured either purple or green. It's not possible to satisfy both of these conditions on the colour of u. This contradiction serves to prove that no planar 6-critical graph exists, so every planar graph is properly 5-colourable. □

In fact, Appel and Haken proved the Four Colour Theorem in 1976.

THEOREM 15.29. Four Colour Theorem *Every planar graph is properly 4-colourable.*

Their proof involved considering a very large number of cases – so many that they used a computer to analyse them all. Although computers are often used in mathematical work now, this was the first proof that could not reasonably be verified by hand. It was viewed with suspicion for a long time, but is now generally accepted.

One of the methods by which mathematicians attempted unsuccessfully to prove the Four Colour Theorem seemed particularly promising, and has led to a lot of interesting work in its own right. We require a couple of definitions to explain the connection.

DEFINITION 15.30. A **cubic graph** is a graph for which all of the vertices have valency 3.

DEFINITION 15.31. A **bridge** in a connected graph is an edge whose deletion disconnects the graph.

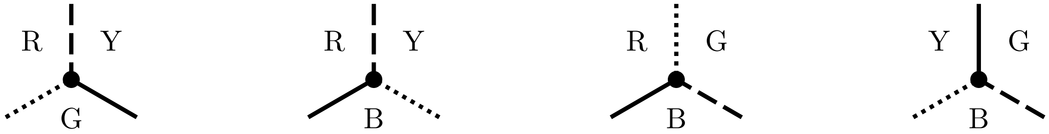
THEOREM 15.32. *The problem of 4-colouring a planar graph is equivalent to the problem of 3-edge-colouring a cubic graph that has no bridges.*

We'll prove one direction of the equivalence stated in this theorem; the other direction is a bit more complicated.

PROOF. Suppose that every planar graph can be properly 4-coloured, and that G is a (simple) bridgeless cubic graph, embedded in the plane. We'll show that there is a proper 3-edge-colouring of G. Since G is bridgeless, we don't run into the problem of a loop in the planar dual, so the Four Colour Theorem applies to the faces of G. Properly colour the faces of G with colours red, green yellow, and black. Every edge of G lies between faces of two distinct colours, by the definition of a proper colouring of a map. Colour the edges of G according to the following table: if the colours of the faces separated by the edge e are the colours listed in the left-hand column, then use the colour listed in the right-hand column to colour e.

Face colours	Edge colour
green, black	dashed
yellow, black	dotted
red, black	solid
green, yellow	solid
green, red	dotted
red, yellow	dashed

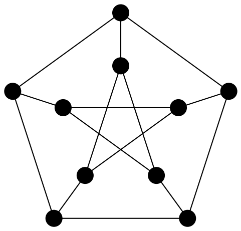
Let v be an arbitrary vertex. We will show that the three edges incident with v must all receive different colours. Since 3 edges meet at v, three faces also meet at v, and every pair of these faces share an edge. Thus the three faces that meet at v must all receive different colours. There are four different cases, depending on which colour is not used for a face at v. We show what happens in the following picture, using R, G, Y, and B to indicate the face colours, and colouring the edges according to the table above in each case.



In each case, the three edges incident with v are assigned different colours, so this is a proper 3-edge colouring of G. □

This theorem was proven by Tait in 1880; he thought that every cubic graph with no bridges must be 3-edge-colourable, and thus that he had proven the Four Colour Theorem. In fact, Vizing's Theorem tells us that any cubic graph can be 4-edge-coloured, so we would only need to reduce the number of colours by 1 in order to prove the Four Colour Theorem. The problem therefore boils down to proving that there are no bridgeless planar cubic graphs that are class two.

In 1881, Petersen published the Petersen graph that we saw previously in Example 14.42.



This graph is cubic and has no bridges, but is not 3-edge-colourable (this can be proved using a case-by-case analysis). Thus, there exist bridgeless cubic graphs that are class two! Many people have tried to find other examples, as classifying these could provide a proof of the Four Colour Theorem.

For many years, Martin Gardner wrote a column in the *Scientific American* about interesting math problems and puzzles. As the Four Colour Theorem is easy to explain without technical language, it was a topic he wrote about. When writing about the importance of bridgeless cubic class two graphs, he decided they needed a more appealing name. Since they seemed rare and elusive, he called them *snarks*, after Lewis Carroll's poem "The Hunting of the Snark." The name has stuck.

DEFINITION 15.33. A **snark** is a bridgeless cubic class two graph.

Two infinite families and a number of individual snarks are known. There is no reason to believe that these are all of the snarks that exist. By the Four Colour Theorem, we know that there are no planar snarks; if we could find a direct proof that there are no planar snarks, this would provide a new proof of the Four Colour Theorem.

EXERCISES 15.34.

1) Prove that if a cubic graph G has a Hamilton cycle, then G is a class one graph.
2) Properly 4-colour the faces of the map given at the start of this section.
3) The map given at the start of this section can be made into a cubic graph, by placing a vertex everywhere two borders meet (including the coast as a border) and edges where there are borders. Use the method from the proof of Theorem 15.32 to properly 3-edge-colour this cubic graph, using your 4-colouring of the faces.
4) Prove that a graph G that admits a planar embedding has an Euler tour if and only if every planar dual of G is bipartite.
5) Prove that if a graph G that admits a planar embedding in which every face is surrounded by exactly 3 edges, G is 3-colourable if and only if it has an Euler tour.

SUMMARY:

- Kuratowski's Theorem, Wagner's Theorem
- Euler's Formula
- $|E| \leq 3|V| - 6$ for a planar graph
- colouring maps
- the Five Colour Theorem
- the Four Colour Theorem
- Important definitions:
  - ○ planar graph, planar embedding
  - ○ face
  - ○ dual graph, planar dual
  - ○ subdividing an edge, subdivision of a graph
  - ○ edge contraction, contracting an edge
  - ○ minor
  - ○ cubic graph
  - ○ bridge
  - ○ snark

Part III

Design Theory

Chapter 16

Latin squares

16A. Latin squares and Sudokus

You can think of a Latin square as a Sudoku puzzle that can be of any (square) size, and does not have the requirement that every value appear in each of the outlined smaller subsquares.

DEFINITION 16.1. A **Latin square** of order n is an $n \times n$ array whose entries are elements of a set N of cardinality n, with the property that every element of N appears exactly once in each row and each column.

EXAMPLE 16.2. Here is a Latin square of order 4:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{array}$$

Notice that in the above example, we placed the numbers $1, 2, 3$, and 4 in the first row, in that order. For each subsequent row, we shifted the numbers one place to the right (wrapping around). This same technique (placing the numbers from 1 through n across the first row) will work to construct a Latin square of order n.

So you might think (with reason) that Latin squares aren't very interesting. However, even knowing that there is a Latin square of every possible order and they are easy to construct, there remain some interesting related questions.

Some of these questions are related to Sudokus. If we fill in some entries of a Latin square, are there conditions on these entries that guarantee that this can be completed to a full Latin square? Are there conditions under which we can be sure that a partial Latin square has a unique completion to a full Latin square?

Some of these questions have easy answers that are not what we are really looking for. For example, if we give you all but one entry of a Latin square (or Sudoku), then if it can be completed at all, the completion will be unique. However, some interesting mathematical work has been done on these problems, both for Latin squares and for Sudokus.

There are no known examples in which a Sudoku puzzle with 16 or fewer squares pre-filled, can be completed uniquely. However, there are tens of thousands of (non-isomorphic) ways of pre-filling 17 entries of a Sudoku puzzle, that have a unique completion. See Gordon Royle's web page `http://staffhome.ecm.uwa.edu.au/~00013890/sudokumin.php` for a complete list of those that are known.

Looking only at "non-isomorphic" examples is important, because there are many ways of creating Latin squares (or Sudoku puzzles) that are essentially the same. The following operations take a Latin square to another Latin square that is structurally essentially the same:

- Permuting of the symbols used in the set N. For example, changing every 1 to a 2 and every 2 to a 1.
- Interchanging any two rows.
- Interchanging any two columns.
- Making all of the rows into columns, and all of the columns into rows.

EXERCISES 16.3.

1) Prove that interchanging two rows of a Latin square, yields a Latin square.
2) Complete the following Latin square. Is the completion unique?

$$\begin{array}{cccc} 1 & \_ & 4 & \_ \\ \_ & 1 & \_ & \_ \\ \_ & \_ & \_ & 3 \\ \_ & \_ & \_ & \_ \end{array}$$

3) Use the method described at the start of this chapter to create a Latin square of order 5. What 3 of the operations listed above that change a Latin square to an isomorphic Latin square, are required to arrive at the following result?

$$\begin{array}{ccccc} 5 & 1 & 4 & 2 & 3 \\ 1 & 3 & 5 & 4 & 2 \\ 4 & 5 & 2 & 3 & 1 \\ 2 & 4 & 3 & 1 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{array}$$

4) Show there are exactly two different Latin squares of order 3 whose first row is $1, 2, 3$.
5) Show there are exactly twelve different Latin squares of order 3 whose entries are the numbers $1, 2, 3$.
[*Hint:* Use Problem 4.]
6) There are four different Latin squares of order 4 whose first row is $1, 2, 3, 4$ and whose first column is also $1, 2, 3, 4$. That is, there are only four ways to complete the following Latin square:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & - & - & - \\ 3 & - & - & - \\ 4 & - & - & - \end{array}$$

Find all four.
[*Hint:* Each of the possibilities for the second entry of the second row can be completed in only one or two ways.]

16B. Mutually orthogonal Latin squares (MOLS)

Most of design theory is concerned with creating nice structures in which different combinations of elements occur equally often. This is the general structure of all of the design theory we will be covering here, and in this context, orthogonal Latin squares are the natural thing to learn about.

DEFINITION 16.4. Two Latin squares S_1 and S_2 are **orthogonal** if when we look at each position in turn and consider the ordered pair formed by the entry of S_1 in that position, and the entry of S_2 in that position, every possible ordered pair appears.

So here, we are looking at positions in the structure of Latin squares, and trying to ensure that every ordered pair appears in each position. Notice that since the set N has n elements, the total number of ordered pairs possible is n^2 (there are n choices for the first entry and n choices for the second entry). A Latin square has n^2 positions since it has n rows and n columns. Thus, if every possible ordered pair appears in each position, then each ordered pair must appear exactly once.

Once again, Euler was involved in the origins of this problem. In fact, the name Latin square comes from his terminology. In 1782, he posed the problem of arranging 36 officers into a 6×6 square. The officers come from 6 different regiments (which he denoted with the Latin characters a, b, c, d, e, and f) and each holds one of 6 possible ranks (which he denoted with the Greek characters α, β, γ, δ, ε, and ζ). No two officers from the same regiment hold the same rank. The question he posed was, is it possible to organise the officers into the square so that in each row and each column, there is precisely one officer from each regiment, and precisely one officer of each rank? Since he was using Greek and Roman letters to denote the classes, he called this a "Graeco-Latin square." He chose the first step to consist of arranging the regiments, i.e. for each regiment to set aside 6 positions in the square to be filled with officers from that regiment. Subsequently, he would try to assign ranks to the officers in these 6 positions. Since the regiments were denoted by Latin characters, he called this first step a "Latin square." The Graeco-Latin square of his question is a pair of orthogonal Latin squares of order 6, since there is to be one officer from each regiment who holds each of the possible ranks.

Euler could not find a solution to this problem. Since there is also no pair of orthogonal Latin squares of order 2 (and possibly for other reasons), he conjectured that there is no pair of orthogonal Latin squares of order n for any $n \equiv 2 \pmod 4$. Although Euler was correct that there is no pair of orthogonal Latin squares of order 6, his conjecture was not true. In 1959–1960, Bose, Shrikhande, and Parker first found constructions for pairs of orthogonal Latin squares of orders 22 and 10, and then found a general construction that can produce a pair of orthogonal Latin squares of order n for every $n > 6$ with $n \equiv 2 \pmod 4$.

EXAMPLE 16.5. Here is a pair of orthogonal Latin squares of order 3:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array} \qquad\qquad \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

We see that the ordered pairs $(1,1)$, $(2,2)$ and $(3,3)$ appear in the first row; the pairs $(3,2)$, $(1,3)$, and $(2,1)$ appear in the second row; and the pairs $(2,3)$, $(3,1)$, and $(1,2)$ appear in the third row. Every possible ordered pair whose entries lie in $\{1,2,3\}$ has appeared.

There is a nice pattern to the squares given in this example. The first follows the general construction we mentioned at the start of this chapter. For the second, each row has been shifted one place to the left (rather than to the right) from the one above it. This construction does actually work for n odd, but never for n even. For example, when $n = 4$, it would give

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{array} \qquad\qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array}$$

You can see that the ordered pair $(1,1)$ occurs in two positions: row 1, column 1, and row 3, column 3. So this pair of Latin squares is definitely not orthogonal. In fact, the first of these squares has no Latin square that is orthogonal to it. However, there is a pair of orthogonal

Latin squares of order 4:

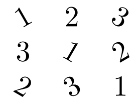
$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array}$$

DEFINITION 16.6. A set of Latin squares is **mutually orthogonal** if *every* distinct pair of Latin squares in the set are orthogonal. We call such a set, a set of MOLS (for Mutually Orthogonal Latin Squares).

The natural question that arises in this context is, how many Latin squares can there be in a set of MOLS?

Before we attempt to answer this question, notice that if we have a pair of orthogonal Latin squares and we permute the symbols used in the set N independently for each of the squares (resulting in new Latin squares that are nonetheless essentially the same, as discussed in Section 16A), the resulting pair of Latin squares will still be orthogonal. If in the first square the symbol x maps to the symbol y, and in the second square the symbol u maps to the symbol v, then in the new pair of Latin squares the ordered pair (y, v) will appear precisely once, since the ordered pair (x, u) appeared precisely once in the original pair of Latin squares. This is true for any pair of entries (y, v), so every pair of entries must appear precisely once.

This idea that we can independently permute the symbols in each square, leads to a very nice method of representing MOLS. The key idea is that it is not necessary to use the *same* set of symbols for each square, since the symbols we choose can be permuted independently to match each other. In fact, we don't need to use symbols at all to represent some of the squares; we can vary some other characteristic. For example, to represent the two orthogonal Latin squares of order 3 that were shown in Example 16.5, we can use the symbols 1 to 3 to represent the first square, and the colours red (for 1), blue (for 2) and green (for 3) to represent the second square. However, varying the colours is not feasible in this textbook, which is printed in black-and-white. Instead, for the second square, let us use "tilted left" (for 1), "straight up" (for 2), and "tilted right" (for 3). So (for example) since in the second row, third column the first square had a 2 and the second had a 1, we place a 2 that is tilted to the left in that location in our new representation (tilted left because the entry of the second square was 1; and 2 because that was the entry of the first square). Here is the complete representation:



By the property of orthogonality, every combination of tilting and number must appear in exactly one position! Even more amazing, if we have a set of MOLS and vary different parameters for each of the squares, the fact that the squares are all mutually orthogonal will mean that every combination of the parameters appears in exactly one position. For example, if we have a set of five MOLS, we could place a coloured shape behind each coloured symbol, and have different numbers of copies of the symbol. For any possible colour of any possible shape appearing behind any possible number of any possible colour of any possible symbol, you would be able to find a position in which that combination appears!

This approach to MOLS is essentially the context in which they first arose, as we can see from Euler's example of the officers. For the two orthogonal Latin squares sought in his question, the symbols in one represent the ranks while the symbols in the other represent the regiment. In his final square, each officer could be represented by a pair of symbols indicating his rank and his regiment – or by a letter for his regiment and a colour for his rank.

Here is a partial answer to the question of how many MOLS of order n there can be:

THEOREM 16.7. *If S is a set of MOLS of order n, then $|S| \leq n - 1$.*

PROOF. We may assume that $N = \{1, \ldots, n\}$. In each of the Latin squares in S, we can independently permute the symbols of N. As was noted above, the result will still be a set of MOLS. We permute the symbols so that the first row of each of the Latin squares has the entries $1, 2, \ldots, n$ in that order.

Now, if we take any $i \in N$ and consider any pair of the Latin squares, the ordered pair (i, i) appears somewhere in the first row. Consider the first entry of the second row in each square of S. None of these entries can be 1, since 1 has already appeared in the first column of each of the Latin squares. No two of the Latin squares can have the same entry j in this position, since the ordered pair (j, j) has already appeared in the jth position of the first row of this pair of squares, so can't appear again in the first position of the second row. So there cannot be more squares in S, than the $n-1$ distinct entries from $N \setminus \{1\}$ that could go into this position. Thus, $|S| \leq n-1$, as claimed. □

The next natural question is, is it possible to achieve $n-1$ MOLS of order n? We have already seen that the answer is yes in one very small case, since we found 2 MOLS of order 3. In fact, there are infinitely many values of n for which there are $n-1$ MOLS of order n.

The following result can be generalised to prime powers using some basic field theory that you should understand if you have taken Math 3400. However, for the purposes of this course, we will avoid the explicit field theory and prove the result only for primes.

We do require a bit of modular arithmetic for this result. As modular arithmetic will also be useful for some of our later results, here is a quick review of some key points.

DEFINITION 16.8. Performing calculations **modulo n** means replacing the result with the remainder you would get upon dividing that result by n. In other words, if the result of a computation is n or larger, replace the result by its remainder upon division by n.

NOTATION 16.9. If a and b have the same remainder upon division by n, then we write $a \equiv b \pmod{n}$.

There are two key facts from modular arithmetic that we will require. The first is that if $a \equiv b \pmod{n}$ and $0 \leq a, b < n$, then we must have $a = b$.

The other is that if $qa \equiv qb \pmod{n}$ and n and q have a greatest common divisor of 1, then $a \equiv b \pmod{n}$. In the special case where n is prime, as long as q is not a multiple of n then n and q will always have a greatest common divisor of 1.

THEOREM 16.10. *For any prime p, there are $p-1$ MOLS of order p.*

PROOF. We will use $N = \{0, \ldots, p-1\}$. In order to ensure that the results of our computations will be in N, all of the calculations given in this result should be taken modulo p.

The squares will be $\{S_1, \ldots, S_{p-1}\}$. For $k \in \{1, \ldots, p\}$,

$$S_k = \begin{bmatrix} 0 & 1 & \ldots & p-1 \\ k & k+1 & \ldots & k+(p-1) \\ 2k & 2k+1 & \ldots & 2k+(p-1) \\ \vdots & \vdots & & \vdots \\ (p-1)k & (p-1)k+1 & \ldots & (p-1)k+(p-1) \end{bmatrix}$$

We first verify that each S_k is a Latin square. The entries in each row are easily seen to be distinct. If the entries in the first column are distinct, then we can see that the entries in every other column will be distinct. Suppose that $0 \leq i, j \leq p-1$ and that $ik \equiv jk \pmod{p}$. Then since every $k \in \{1, \ldots, p-1\}$ has a greatest common divisor of 1 with p, we see that $i \equiv j \pmod{p}$. Since $0 \leq i, j \leq p-1$, this forces $i = j$. So the entries in the first column of S_k are all distinct. Thus, every S_k is a Latin square.

Suppose that for some $1 \leq i, j \leq p-1$, the squares S_i and S_j have the same ordered pair in two positions: row k_1, column m_1, and row k_2, column m_2. Then by the formulas given for the entries of each Latin square, we must have

$$\begin{array}{rcl} (k_1-1)i+m_1-1 & \equiv & (k_2-1)i+m_2-1 \pmod{p}, \\ \text{and } (k_1-1)j+m_1-1 & \equiv & (k_2-1)j+m_2-1 \pmod{p}. \\ \text{Thus, } k_1i+m_1 & \equiv & k_2i+m_2 \pmod{p}, \\ \text{and } k_1j+m_1 & \equiv & k_2j+m_2 \pmod{p}. \\ \text{Therefore, } m_2-m_1 \equiv k_2i-k_1i & = & (k_2-k_1)i \equiv k_2j-k_1j = (k_2-k_1)j \pmod{p}. \end{array}$$

Since $(k_2-k_1)i \equiv (k_2-k_1)j \pmod{p}$, and $1 \leq i, j \leq p-1$, either $i = j$ (so we chose the same Latin square twice instead of choosing a pair of distinct Latin squares), or $k_2 - k_1 \equiv 0 \pmod{p}$. Since k_1 and k_2 are row numbers, they are between 1 and p so this forces $k_1 = k_2$. Furthermore, in this case we must also have $m_2 - m_1 \equiv 0 \pmod{p}$, and we see that this also forces $m_1 = m_2$. Thus, the two positions in which the same ordered pair appeared, were actually the same position chosen twice.

This shows that $\{S_k \mid 1 \leq k \leq p-1\}$ is indeed a set of $p-1$ MOLS. □

EXAMPLE 16.11. Here are the first 8 of the 10 MOLS of order 11, found using the formula given in the proof above.

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

0	1	2	3	4	5	6	7	8	9	10
2	3	4	5	6	7	8	9	10	0	1
4	5	6	7	8	9	10	0	1	2	3
6	7	8	9	10	0	1	2	3	4	5
8	9	10	0	1	2	3	4	5	6	7
10	0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	10	0
3	4	5	6	7	8	9	10	0	1	2
5	6	7	8	9	10	0	1	2	3	4
7	8	9	10	0	1	2	3	4	5	6
9	10	0	1	2	3	4	5	6	7	8

0	1	2	3	4	5	6	7	8	9	10
3	4	5	6	7	8	9	10	0	1	2
6	7	8	9	10	0	1	2	3	4	5
9	10	0	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	9	10	0
4	5	6	7	8	9	10	0	1	2	3
7	8	9	10	0	1	2	3	4	5	6
10	0	1	2	3	4	5	6	7	8	9
2	3	4	5	6	7	8	9	10	0	1
5	6	7	8	9	10	0	1	2	3	4
8	9	10	0	1	2	3	4	5	6	7

0	1	2	3	4	5	6	7	8	9	10
4	5	6	7	8	9	10	0	1	2	3
8	9	10	0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8	9	10	0
5	6	7	8	9	10	0	1	2	3	4
9	10	0	1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	9	10	0	1
6	7	8	9	10	0	1	2	3	4	5
10	0	1	2	3	4	5	6	7	8	9
3	4	5	6	7	8	9	10	0	1	2
7	8	9	10	0	1	2	3	4	5	6

0	1	2	3	4	5	6	7	8	9	10
5	6	7	8	9	10	0	1	2	3	4
10	0	1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	10	0	1	2	3
9	10	0	1	2	3	4	5	6	7	8
3	4	5	6	7	8	9	10	0	1	2
8	9	10	0	1	2	3	4	5	6	7
2	3	4	5	6	7	8	9	10	0	1
7	8	9	10	0	1	2	3	4	5	6
1	2	3	4	5	6	7	8	9	10	0
6	7	8	9	10	0	1	2	3	4	5

0	1	2	3	4	5	6	7	8	9	10
6	7	8	9	10	0	1	2	3	4	5
1	2	3	4	5	6	7	8	9	10	0
7	8	9	10	0	1	2	3	4	5	6
2	3	4	5	6	7	8	9	10	0	1
8	9	10	0	1	2	3	4	5	6	7
3	4	5	6	7	8	9	10	0	1	2
9	10	0	1	2	3	4	5	6	7	8
4	5	6	7	8	9	10	0	1	2	3
10	0	1	2	3	4	5	6	7	8	9
5	6	7	8	9	10	0	1	2	3	4

0	1	2	3	4	5	6	7	8	9	10
7	8	9	10	0	1	2	3	4	5	6
3	4	5	6	7	8	9	10	0	1	2
10	0	1	2	3	4	5	6	7	8	9
6	7	8	9	10	0	1	2	3	4	5
2	3	4	5	6	7	8	9	10	0	1
9	10	0	1	2	3	4	5	6	7	8
5	6	7	8	9	10	0	1	2	3	4
1	2	3	4	5	6	7	8	9	10	0
8	9	10	0	1	2	3	4	5	6	7
4	5	6	7	8	9	10	0	1	2	3

0	1	2	3	4	5	6	7	8	9	10
8	9	10	0	1	2	3	4	5	6	7
5	6	7	8	9	10	0	1	2	3	4
2	3	4	5	6	7	8	9	10	0	1
10	0	1	2	3	4	5	6	7	8	9
7	8	9	10	0	1	2	3	4	5	6
4	5	6	7	8	9	10	0	1	2	3
1	2	3	4	5	6	7	8	9	10	0
9	10	0	1	2	3	4	5	6	7	8
6	7	8	9	10	0	1	2	3	4	5
3	4	5	6	7	8	9	10	0	1	2

We've now seen that it is possible to find $p-1$ MOLS of order p for any prime p, and that the proof can be generalised to prime powers. However, as we've already discussed in relation to Euler's original problem, there are orders for which the bound of $n-1$ MOLS of order n cannot be attained: in fact, for order 6 it is not possible even to find a pair of orthogonal Latin squares.

If you are interested in or familiar with some finite geometry, the existence of $n-1$ MOLS of order n is equivalent to the existence of a projective plane of order n. Projective planes, in turn, are a special kind of design. For an interesting article about some of these relationships, see `https://www.maa.org/sites/default/files/pdf/upload_library/22/Ford/Lam305-318.pdf`. There is also some information about this in Sections 18C and 18D.

EXERCISES 16.12.

1) Find the two MOLS of order 11 that are not included in Example 16.11, but are orthogonal to each other and to the squares listed there.
2) Find a third Latin square of order 4 that is orthogonal to both of the orthogonal Latin squares of order 4 that were given earlier in this section.
3) Here is a Latin square of order 8, and some entries for a second Latin square of order 8. Complete the second square so as to obtain a pair of orthogonal Latin squares.

1	2	3	4	5	6	7	8
2	1	4	3	6	5	8	7
3	4	1	2	7	8	5	6
4	3	2	1	8	7	6	5
5	6	7	8	1	2	3	4
6	5	8	7	2	1	4	3
7	8	5	6	3	4	1	2
8	7	6	5	4	3	2	1

1	2	3	4	5	6	7	8
3	4	_	_	_	8	5	6
5	_	7	_	_	2	3	_
7	_	_	6	_	_	_	_
4	_	_	1	8	_	_	_
2	_	_	_	_	5	_	_
8	_	_	_	_	_	_	1
6	_	_	7	_	_	_	3

4) Write down the six mutually orthogonal Latin squares $S_1, \dots, S_6$ of order 7 that are constructed by letting $p = 7$ in the proof of Theorem 16.10.

16C. Systems of distinct representatives

Suppose we start filling in a Latin square, one row at a time, at each step ensuring that no element has yet appeared more than once in a column (or in a row). Under what conditions will it be impossible to complete this to a Latin square? Although it may not be immediately obvious, the answer to this question can be found in a well-known theorem published by Philip Hall in 1935, about systems of distinct representatives.

DEFINITION 16.13. Let $T_1 \dots, T_n$ be sets. If there exist $a_1, \dots, a_n$ all distinct such that for every $1 \leq i \leq n$, $a_i \in T_i$, then $\{a_1, \dots a_n\}$ form a **system of distinct representatives (SDR)** for $T_1, \dots, T_n$.

EXAMPLE 16.14. The university is striking a student committee on the subject of tutorials. For each of the 5 Faculties, they ask students to elect one representative who is taking classes from that faculty. They do not want one student trying to represent more than one faculty. The candidates are:

- Joseph, who is taking courses in Arts and Science, Fine Arts, Management, and Education;
- René, who is taking courses in Health Sciences;
- Claire, who is taking courses in Education and Health Sciences;
- Sandra, who is taking courses in Management, Fine Arts, and Health Sciences;
- Laci, who is taking courses in Education and Health Sciences; and
- Jing, who is taking courses in Education.

Can the committee be filled?

SOLUTION. The answer is no. For the three Faculties of Arts & Science, Fine Arts, and Management, there are only two possible student representatives: Joseph (who could represent any of the three), and Sandra (who could represent either Fine Arts or Management). So it is not possible to elect one student to represent each of the five Faculties, without allowing one of these students to fill two roles. □

In Example 16.14, we observed that we could find a collection of the sets to be represented, that collectively had fewer possible representatives than there are sets in the collection. It is easy to see that if this happens, there cannot be a system of distinct representatives for the sets.

What Philip Hall proved is the converse: unless we have an obstruction of this type, it is always possible to fine a system of distinct representatives.

THEOREM 16.15. Hall's Theorem *The collection of sets $T_1, \dots, T_n$ has a system of distinct representatives if and only if for every $1 \leq k \leq n$, the union of any k of the sets has cardinality at least k.*

This theorem is often referred to as "Hall's Marriage Theorem," as one of the problems it solves can be stated as follows. Suppose we have a collection of men and a collection of women. Each of the women has a list of men she likes (from the collection). When is it possible to marry each of the women to a man that she likes? (The context is historical, and the assumption of the time was that every woman would want to marry a man.)

We have seen that one of the two implications of Hall's Theorem is easy to prove. We will not try to prove the other implication here, but will focus on using the result. Here are some examples and exercises. For completeness, we provide a proof of Hall's Theorem at the end of this chapter.

EXAMPLE 16.16. Let $A_1 = \{a, b, c, d\}$, $A_2 = \{b, c\}$, $A_3 = \{b\}$, $A_4 = \{b, c\}$. Does this collection of sets have a system of distinct representatives? If so, find one; if not, explain why.

SOLUTION. The answer is that this collection of sets has no system of distinct representatives, because the union of three sets A_2, A_3, and A_4 has only two elements: b and c. □

EXAMPLE 16.17. Let $A_1 = \{a, d\}$, $A_2 = \{a, c\}$, $A_3 = \{b, c\}$, $A_4 = \{c, d\}$. Does this collection of sets have a system of distinct representatives? If so, find one; if not, explain why.

SOLUTION. This collection of sets does have a system of distinct representatives: take a for A_1, c for A_2, b for A_3, and d for A_4. For clarity, we underline the representatives in the following list of the sets: $A_1 = \{\underline{a}, d\}$, $A_2 = \{a, \underline{c}\}$, $A_3 = \{\underline{b}, c\}$, $A_4 = \{c, \underline{d}\}$.

(In fact, it also has another system of distinct representatives: take d for A_1, a for A_2, b for A_3, and c for A_4: $A_1 = \{a, \underline{d}\}$, $A_2 = \{\underline{a}, c\}$, $A_3 = \{\underline{b}, c\}$, $A_4 = \{\underline{c}, d\}$.) □

EXERCISES 16.18. For each collection of sets, determine whether or not it has a system of distinct representatives. If so, find one; if not, explain why.

1) $A_1 = \{x\}$, $A_2 = \{y, z\}$, $A_3 = \{x, y\}$.
2) $A_1 = \{u, v, w, x, y, z\}$, $A_2 = \{v, w, y\}$, $A_3 = \{w, x, y\}$, $A_4 = \{v, w, x, y\}$, $A_5 = \{v, x, y\}$, $A_6 = \{v, y\}$.
3) $A_1 = \{x\}$, $A_2 = \{y\}$, $A_3 = \emptyset$.
4) $A_1 = \{x, z\}$, $A_2 = \{y\}$, $A_3 = \{x, y, z\}$.
5) $T_1 = \{a, b, c, d\}$, $T_2 = \{a, b, c\}$, $T_3 = \{a\}$, $T_4 = \{c\}$.
6) $U_1 = \{x, y\}$, $U_2 = \{y, z\}$, $U_3 = \emptyset$.
7) $V_1 = \{e, f\}$, $V_2 = \{e, g\}$, $V_3 = \{e, h\}$, $V_4 = \{f, g\}$, $V_5 = \{h, i\}$.
8) $W_1 = \{+, -, \times, \div, 0\}$, $W_2 = \{+, -, \times\}$, $W_3 = \{+, \times\}$, $W_4 = \{\times, -\}$, $W_5 = \{+, -\}$.

Let's return to our original question about Latin squares. To answer this, we first give an important general consequence of Hall's Theorem.

PROPOSITION 16.19. *Suppose $T_1, \ldots, T_n$ is a collection of sets each of which contains exactly r elements. Further suppose that no element appears in more than r of the sets. Then this collection has a system of distinct representatives.*

PROOF. By Hall's Theorem, we must show that for every $1 \leq k \leq n$, the union of any k of the sets $T_1, \ldots, T_n$ has cardinality at least k. Let $k \in \{1, \ldots, n\}$ be arbitrary, and arbitrarily choose k of the sets $T_{j_1}, \ldots T_{j_k}$. If $k \leq r$ then since each T_{j_i} has r elements, their union must have at least $r \geq k$ elements, as desired.

Suppose on the other hand that $k > r$. Amongst the k sets of r elements, a total of kr elements appear (counting each element every time it appears). Since each element appears in at most r of the sets, it must be the case that at least k distinct elements appear. This completes the proof. □

We can now answer the question about Latin squares.

THEOREM 16.20. *Suppose that m rows of a Latin square of order n have been filled, where $m < n$, and that to this point no entry appears more than once in any row or column. Then another row can be added to the Latin square, maintaining the condition that no entry appears more than once in any row or column.*

PROOF. For $1 \leq i \leq n$, let T_i be the set of elements that have not yet appeared in column i (from the entries in the first m rows). So T_i can be thought of as the set of allowable entries for the ith column of the new row. Notice that each T_i has cardinality $n - m$ (the number of rows that are still empty). The task of finding a new row all of whose entries are distinct, and whose ith entry comes from the set T_i of allowable entries for that column, is equivalent to finding a system of distinct representatives for the sets $T_1, \ldots, T_n$. Thus, we must show that the collection $T_1, \ldots, T_n$ has a system of distinct representatives.

Notice also that every element has appeared once in each of the first m rows, and thus has appeared in precisely m of the columns. Therefore, there are exactly $n - m$ of the columns in which it has not yet appeared. In other words, each element appears in exactly $n - m$ of the sets.

We can now apply Proposition 16.19, with $r = n - m$ to see that our sets do have a system of distinct representatives. This can be used to form a new row for the Latin square. □

COROLLARY 16.21. *Suppose that m rows of a Latin square of order n have been filled, where $m < n$, and that to this point no entry appears more than once in any row or column. This structure can always be completed to a Latin square.*

PROOF. As long as $m < n$, we can repeatedly apply Theorem 16.20 to deduce that it is possible to add a row. Once you actually find a row that can be added (note that the statement of Hall's Theorem does not explain how to do this), do so. Eventually this process will result in a complete square. □

Hall's Theorem can also be used to prove a special case of a result we proved previously, Theorem 14.17. The special case we can prove with Hall's Theorem, is the case where every vertex has the same valency.

THEOREM 16.22. *If G is a bipartite graph in which every vertex has the same valency, then any bipartition sets V_1 and V_2 have the same cardinality, and there is a set of $|V_1|$ edges that can be properly coloured with the same colour.*

PROOF. Let k be the valency of every vertex, and for some arbitrary bipartition sets V_1 and V_2, let $n = |V_1|$. By a slight adaptation of Euler's handshaking lemma, taking into account the fact that every edge has exactly one of its endvertices in V_1, we see that $nk = |E|$. By the same argument, $k|V_2| = |E|$, which forces $|V_2| = n = |V_1|$. Since the bipartition was arbitrary, the first statement follows.

Let $V_1 = \{v_1, \ldots, v_n\}$. For every $1 \leq i \leq n$, let

$$T_i = \{u \in V \mid u \sim v_i\}.$$

A system of distinct representatives for the sets $T_1, \ldots, T_n$ will produce $n = |V_1|$ edges that can be properly coloured with the same colour.

Observe that every set T_i has cardinality k (since this is the valency of every vertex), and every vertex appears in exactly k of the sets (again because this is the valency of the vertex). Therefore, by Proposition 16.19, there is a system of distinct representatives for $T_1, \ldots, T_n$. Hence we can find $n = |V_1|$ edges that can be properly coloured with the same colour. □

COROLLARY 16.23. *If G is a bipartite graph in which every vertex has the same valency k, then its edges can be properly coloured using k colours.*

PROOF. Repeat the following step k times: find a set of edges that can be properly coloured. Colour them with a new colour, and delete them from the graph.

At each stage, Theorem 16.22 tells us providing that every vertex has the same valency, we can find a set of edges that are properly coloured, one of which is incident with every vertex of the graph. Since the valency of every vertex is reduced by exactly one when we delete such a set of edges, at each stage every vertex will have the same valency. □

To conclude the chapter, we provide a proof of Hall's Theorem. As previously noted, one direction is obvious, so we prove only the other direction.

THEOREM 16.24 Hall's Theorem. *The collection of sets $T_1, \ldots, T_n$ has a system of distinct representatives if for every $1 \leq k \leq n$, the union of any k of the sets has cardinality at least k.*

PROOF. We will prove this by strong induction on the number of sets, n.

Base case: $n = 1$. If a single set has one element, then that set has a representative. This completes the proof of the base case.

Inductive step: We begin with the inductive hypothesis. Let $m \geq 1$ be arbitrary. Suppose that whenever $1 \leq i \leq m$, and a collection of i sets $T_1, \ldots, T_i$ has the property that for every $1 \leq k \leq i$, the union of any k of the sets has cardinality at least k, then that collection of sets has a system of distinct representatives.

We want to deduce that whenever we have a collection of $m+1$ sets with the property that for every $1 \leq k \leq m+1$, the union of any k of the sets has cardinality at least k, then that collection of sets has a system of distinct representatives. Let $T_1, \ldots, T_{m+1}$ be such a collection of sets.

We look at the subcollection of sets $T_1, \ldots, T_m$, and consider two cases. First, suppose that for every $1 \leq k \leq m$, the union of any k of these sets has cardinality at least $k+1$. In this case, take any element $t \in T_{m+1}$ (which by hypothesis is nonempty) to be the representative for T_{m+1}, and remove this element from each of the other sets. Due to the case we are in, for every $1 \leq k \leq m$, the union of any k of the sets $T_1 - \{t\}, \ldots, T_m - \{t\}$ still has cardinality at least k, (we have removed only the element t from this union, which previously had cardinality at least $k+1$). Thus we can apply our induction hypothesis to find a system of distinct representatives for $T_1, \ldots, T_m$ that does not include the element t. This completes a system of distinct representatives for our full collection of sets.

The other case is that there is some $1 \leq k \leq m$ and some collection of k of the sets $T_1, \ldots, T_m$, whose union has cardinality precisely k. By our induction hypothesis, there is a system of distinct representatives for these k sets. From the other $m+1-k$ sets (observe that $1 \leq m+1-k \leq m$), remove the k elements that were in the union of the original k sets. Consider any k' of these adjusted sets, with $1 \leq k' \leq m+1-k$. Observe that the union of the $k+k'$ sets consisting of the original k sets together with these k' sets must have contained at least $k+k'$ distinct elements by hypothesis, so after removing the k representatives of the original k sets (which are the only elements in those sets), these k' sets must still have at least k' distinct elements in their union. Therefore, we can apply our induction hypothesis to these other $m+1-k$ adjusted sets, and see that they too have a system of distinct representatives, none of which are amongst the k representatives for the original k sets. Combining these two systems of distinct representatives yields a system of distinct representatives for the full collection of sets. □

EXERCISES 16.25.

1) Onyx is doing some research on what people learn from visiting different countries. She has a set of questions that are to be answered by someone who has visited the country. Before fully launching the study, she wants to try the questions out on some of her friends. Since the questions are the same for different countries, she doesn't want one person to answer the questions for more than one country, as that could bias the results. Of her close friends, the following people have visited the following countries:

   - England: Adam, Ella, Justin
   - Wales: Adam, Justin, Faith, Cayla
   - Scotland: Bryant, Justin, Ella
   - Ireland: Adam, Bryant, Justin
   - Germany: Cayla, Bryant, Justin, Faith, Denise
   - France: Ella, Justin, Bryant
   - Italy: Adam, Ella, Bryant

   Prove that Onyx cannot find seven different friends, each of whom has visited a different one of these countries.

2) Can the following be completed to a 4×4 Latin square? Does Hall's Theorem apply to this? If not, why not?

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 2 & 4 & & \end{array}$$

3) Show (by example) that it is possible to have a bipartite graph in which the bipartition sets have the same cardinality k and the valency of every vertex is either 3 or 4, but no set of k edges can be properly coloured with a single colour.

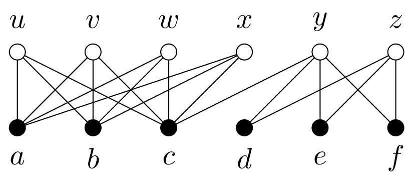
4) How do you know (without actually finding a completion) that the following can be completed to a Latin square of order 7?

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & 6 & 1 & 5 & 3 \\ 3 & 7 & 4 & 2 & 6 & 1 & 5 \\ 4 & 6 & 2 & 5 & 3 & 7 & 1 \end{array}$$

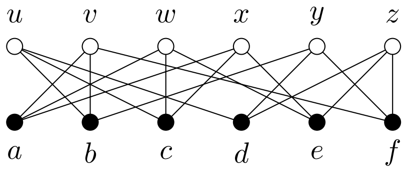
5) Find a completion of the partial Latin square in Problem 4.

6) For each of these bipartite graphs, let $V_1 = \{a, b, c, d, e, f\}$, and determine whether there is a set of $|V_1|$ disjoint edges. (In other words, determine whether there is a set of $|V_1|$ edges that can be properly coloured with the same colour.)

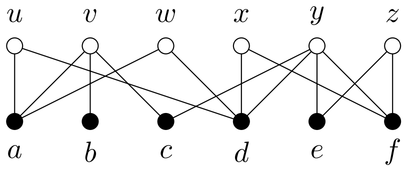
   (a)



(b)



(c)



SUMMARY:

- Hall's (Marriage) Theorem
- a partial Latin square containing m rows can always be completed.
- Important definitions:
  - Latin square
  - orthogonal Latin squares
  - MOLS (mutually orthogonal Latin squares)
  - system of distinct representatives (SDR)

Chapter 17

Designs

17A. Balanced Incomplete Block Designs (BIBD)

Suppose you have 7 possible treatments for a disease, that you hope may work well singly or in combination. You would like to try out every possible combination of them, but the number of (non-empty) subsets of the set of 7 treatments is $2^7 - 1 = 127$, and you have only 7 mice in the lab who have this disease. You believe that using a pair of the treatments together will have a more significant impact than adding more of the treatments, but even trying every pair of treatments on a different mouse would require $\binom{7}{2} = 21$ mice.

Here is a strategy you could try: give each of the mice 3 of the treatments, according to the following scheme. For $1 \le i \le 7$, the treatments given to mouse i will be the elements of the ith set in the following list:

$$\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}.$$

Careful perusal of this scheme will show that every pair of treatments is used together on precisely one of the mice.

DEFINITION 17.1. A **design** is a pair $(V, \mathcal{B})$, where V is a finite set of points (varieties) and $\mathcal{B}$ is a collection of subsets of V, called **blocks** of the design.

This definition of a design is too broad to be of much interest without additional constraints, but a variety of different constraints have been studied.

NOTATION 17.2. We use v to denote $|V|$ and b to denote $|\mathcal{B}|$.

DEFINITION 17.3. A **regular** design is a design in which every point appears in the same number of blocks, r.

A **uniform** design is a design in which every block contains the same number of points, k.

A **balanced** design is a design in which every pair of points appear together in the same number of blocks, λ.

EXAMPLE 17.4. In our disease treatments for the mice, we have $V = \{1,2,3,4,5,6,7\}$,

$$\mathcal{B} = \{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}\}.$$

This is a regular, uniform, balanced design. In this design, $v = 7$, $b = 7$, $r = 3$, $k = 3$, and $\lambda = 1$.

A regular, uniform, balanced design may be referred to as a (b, v, r, k, λ)-design. So our disease treatments for the mice formed a $(7, 7, 3, 3, 1)$-design.

A (b, v, r, k, λ)-design is called *complete* if $v = k$. In this case, every block will contain every point. A (b, v, r, k, λ)-design is called *trivial* if $k = 1$. In this case, every block consists of a single point, and no points appear together in a block. The case $k = 2$ is also fairly trivial since in this case the blocks of the design must consist of the $\binom{v}{2}$ pairs of elements of v, each occurring λ times.

DEFINITION 17.5. A **balanced incomplete block design (BIBD)** is a regular, uniform, balanced design that is not complete. So it is a (b, v, r, k, λ)-design with $k < v$.

Although this definition includes the possibility $k = 1$ or $k = 2$, these are not interesting cases, and can usually be ignored.

EXAMPLE 17.6. Here is another BIBD. This one has parameters $(20, 16, 5, 4, 1)$.

$$\{a, b, c, d\},\quad \{e, f, g, h\},\quad \{i, j, k, l\},\quad \{m, n, o, p\},\quad \{a, e, i, m\},\quad \{a, f, j, n\},\quad \{a, g, k, o\},$$
$$\{a, h, l, p\},\quad \{b, e, j, o\},\quad \{b, f, i, p\},\quad \{b, g, l, m\},\quad \{b, h, k, n\},\quad \{c, e, l, o\},\quad \{c, f, k, p\},$$
$$\{c, g, i, n\},\quad \{c, h, j, m\},\quad \{d, e, k, n\},\quad \{d, f, l, m\},\quad \{d, g, j, p\},\quad \{d, h, i, o\}$$

THEOREM 17.7. *If a (b, v, r, k, λ)-design exists, then $bk = vr$ and*

$$r(k-1) = \lambda(v-1).$$

COMBINATORIAL PROOF. For the first equation, we count the total number of appearances of each point in the design (including repetitions) in two ways. This is another example of counting ordered pairs from a cartesian product, as we have discussed previously.

First, there are b blocks, each of which has k points in it. So the answer will be bk.

Second, there are v points, each of which appears r times. So the answer will be vr.

Thus, $vr = bk$.

For the second equation, we fix a point p, and count the number of points with which p appears in a block, in two ways.

First, p appears in r blocks. In each of these, there are $k-1$ points besides p. So the answer will be $r(k-1)$.

Second, for every point $p' \in V$ with $p' \neq p$, the point p' appears with p in λ different blocks. Since there are $v-1$ choices for p', the answer will be $\lambda(v-1)$.

Thus, $r(k-1) = \lambda(v-1)$. □

With a bit of calculation, the results of Theorem 17.7 tell us that:

$$r = \frac{\lambda(v-1)}{k-1} \tag{17.8}$$

and

$$b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)} \tag{17.9}$$

Thus, if we know that a design is regular, uniform, and balanced, then the parameters r and b can be determined from the parameters v, k, and λ. We therefore often shorten our notation and refer to a BIBD(v, k, λ).

THEOREM 17.10. *A BIBD(v, k, λ) is equivalent to colouring the edges of the multigraph λK_v (the multigraph in which each edge of K_v has been replaced by λ copies of that edge) so that the edges of any colour form a K_k.*

PROOF. Given an edge-colouring of λK_v as described, define the points of the design to be the set of vertices of the multigraph, and for each colour, create a block whose vertices are the vertices of the K_k that has that colour. All of these blocks will have cardinality k. Every vertex has valency $\lambda(v-1)$, and every K_k of one colour that contains that vertex will use $k-1$ of the edges incident with that vertex, so every vertex will appear in

$$r = \lambda(v-1)/(k-1)$$

blocks. Now, any edge of the λK_v must appear in some K_k (the one coloured with the colour of that edge). Thus for any pair of points, these vertices are joined by λ edges each of which appears in some K_k, so these points must appear together in λ of the K_k subgraphs, i.e λ of the blocks.

Similarly, given a BIBD(v, k, λ), and a multigraph λK_v, label the vertices of K_v with the points of the design. For each block of the design, use a new colour to colour the edges of a K_k that connects the points in that block. There will be enough uncoloured edges joining these points, since every pair of points appear together in exactly λ blocks, and there are λ edges joining the corresponding vertices. In fact, careful counting can show that this will result in colouring every edge of the multigraph. □

This is nicest in the case where $\lambda = 1$, when the BIBD corresponds to an edge-colouring of K_v.

A colouring of the edges of a graph (or multigraph) is often referred to as a *decomposition* of the graph (or multigraph), since we can think of the colour classes as sets of edges whose union forms the entire edge set of the graph.

These provide alternate ways of thinking of designs that may be more intuitive, and are certainly more visual.

Equations (17.8) and (17.9) lead to numerical conditions on v, k, and λ that must be satisfied in order for a BIBD(v, k, λ) to exist.

THEOREM 17.11. *A BIBD(v, k, λ) cannot exist unless*

$$\lambda\frac{v-1}{k-1} \quad \textit{and} \quad \lambda\frac{v(v-1)}{k(k-1)}$$

are integers.

PROOF. By Equation (17.8), every point of the design must appear in

$$\lambda(v-1)/(k-1)$$

blocks. Since a point can only appear in an integral number of blocks, the first result follows.

Similarly, By Equation (17.9), there must be

$$\frac{\lambda v(v-1)}{k(k-1)}$$

blocks in the design. Since there can't be a fractional number of blocks, the second result follows. □

Although these conditions are necessary to the existence of a BIBD, there is no guarantee that a BIBD with specified parameters will exist, even if those parameters satisfy these conditions.

EXAMPLE 17.12. The parameters $v = 15$, $k = 5$, $\lambda = 2$ satisfy the conditions of Theorem 17.11, but there is no BIBD$(15, 5, 2)$.

We will not prove that such a design does not exist as the proof would be tedious and unenlightening. We will verify that the parameters satisfy the necessary conditions.

We have

$$\lambda(v-1)/(k-1) = 2(14)/4 = 7,$$

and

$$\frac{\lambda v(v-1)}{k(k-1)} = 2 \cdot 15 \cdot 14/20 = 21.$$

Both of these are integers, so if a design were to exist, each point would appear in 7 blocks, and there would be 21 blocks. A computer search can verify that no such design exists.

EXERCISES 17.13.

1) Show that for any BIBD(v, k, λ), the number of edges of λK_v is equal to the number of edges of K_k times the number of blocks of the design.

2) Suppose there is a BIBD$(16, 6, 3)$. How many blocks does it have? In how many of those blocks does each point appear?

3) Find an edge-colouring of K_5 so that the edges of any colour form a K_2. What are the parameters of the design to which this corresponds?

4) Here are the blocks of a BIBD with $\lambda = 1$:

$$\begin{array}{llll} B_1 = \{1,2,3\} & B_2 = \{1,4,7\} & B_3 = \{1,5,9\} & B_4 = \{1,6,8\} \\ B_5 = \{4,5,6\} & B_6 = \{2,5,8\} & B_7 = \{2,6,7\} & B_8 = \{2,4,9\} \\ B_9 = \{7,8,9\} & B_{10} = \{3,6,9\} & B_{11} = \{3,4,8\} & B_{12} = \{3,5,7\}. \end{array}$$

(a) What are the values of v, b, k, and r for this BIBD?

(b) How many of the blocks contain the element 7 ?

(c) How many of the blocks contain both 2 and 7 ?

(d) Which blocks contain the element 5 ?

(e) Which blocks contain both 5 and 8 ?

5) Assume $\mathcal{B}$ is a BIBD with $v = 16$, $k = 4$, and $r = 3$.

(a) What are the values of b and λ?

(b) Can you tell whether such a BIBD exists or not?

6) A prize draw allows you to enter by picking 3 numbers from $\{1, \ldots, 14\}$. You will win a prize if you choose two of the three numbers that they will draw. Show that it is possible to guarantee a win by having 14 entries in the draw. Explain whether or not a similar strategy would work if the numbers were chosen from $\{1, \ldots, 21\}$.
[*Hint:* Use the $(7, 7, 3, 3, 1)$ design.]

17B. Constructing designs, and existence of designs

There are a number of nice methods for constructing designs. We will discuss some of these methods in this section. For some of them, you must start with one design, and use it to create a different design.

Method 1: Repeating blocks

This is probably the easiest, and (not surprisingly) the least useful of our construction methods.

Start with a BIBD(v, k, λ). For each block of the design, create t copies of that block. The result will be a BIBD$(v, k, t\lambda)$.

Method 2: Taking the complement

This method also requires starting with a design. Start with $(V, \mathcal{B})$, a BIBD(v, k, λ).

Replace each block $B \in \mathcal{B}$ with its complementary block, $B^c = V \setminus B$. Then

$$(V, \{B^c \mid B \in \mathcal{B}\})$$

is a design.

DEFINITION 17.14. We call the design constructed by this method, the **complementary design** or **complement** of the design we started with.

PROPOSITION 17.15. *The complement of a BIBD(v, k, λ) is a BIBD$(v, v-k, b-2r+\lambda)$.*

The proof of this proposition is left to the reader, as Exercise 17.20(1).

EXAMPLE 17.16. The complement of the design given in Example 17.6, is the following:

$$\begin{array}{cc}
\{e,f,g,h,i,j,k,l,m,n,o,p\}, & \{a,b,c,d,i,j,k,l,m,n,o,p\} \\
\{a,b,c,d,e,f,g,h,m,n,o,p\}, & \{a,b,c,d,e,f,g,h,i,j,k,l\} \\
\{b,c,d,f,g,h,j,k,l,n,o,p\}, & \{b,c,d,e,g,h,i,k,l,m,o,p\} \\
\{b,c,d,e,f,h,i,j,l,m,n,p\}, & \{b,c,d,e,f,g,i,j,k,m,n,o\} \\
\{a,c,d,f,g,h,i,k,l,m,n,p\}, & \{a,c,d,e,g,h,j.k.l,m,n,o\} \\
\{a,c,d,e,f,h,i,j,k,n,o,p\}, & \{a,c,d,e,f,g,i,j,l,m,o,p\} \\
\{a,b,d,f,g,h,i,j,k,m,n,p\}, & \{a,b,d,e,g,h,i,j,l,m,n,o\} \\
\{a,b,d,e,f,h,j,k,l,m,o,p\}, & \{a,b,d,e,f,g,i,k,l,n,o,p\} \\
\{a,b,c,e,g,h,i,j,k,n,o,p\}, & \{a,b,c,e,g,h,i,j,k,n,o,p\} \\
\{a,b,c,e,f,h,i,k,l,m,n,o\}, & \{a,b,c,e,f,g,j,k,l,m,n,p\}
\end{array}$$

Its parameters are $b = 20$, $v = 16$, $r = 15$, $k = 12$, $\lambda = 11$.

Method 3: Cyclic designs

This method may be easiest to think of in terms of the associated graph colouring. There are various more complicated versions of this construction that enable us to construct additional designs, but for the purposes of this course, we will focus on the most basic version. This most basic version unfortunately only works when v is odd.

DEFINITION 17.17. Fix an odd integer n. A collection of sets $D_1, \ldots, D_m \subseteq \{1, \ldots, n\}$ is a **difference collection** for n, if taking the differences $j - i$ for every pair $i \neq j$ with $i, j \in D_k$ for each set D_k, attains each of the values $\pm 1, \ldots, \pm(n-1)/2$, exactly once, when computations are performed modulo n. If $m = 1$ then D_1 is called a **difference set**.

EXAMPLE 17.18. The collection $\{1, 2, 5\}, \{1, 3, 10\}, \{1, 7, 15\}$ is a difference collection for $n = 19$. The differences we attain appear in the following table.

Difference set	i	j	$j-i, i-j$
D_1	1	2	± 1
D_1	1	5	± 4
D_1	2	5	± 3
D_2	1	3	± 2
D_2	1	10	± 9
D_2	3	10	± 7
D_3	1	7	± 6
D_3	1	15	$\pm 14 \equiv \pm 5 \pmod{19}$
D_3	7	15	± 8

Suppose we have a difference collection for v in which each set $D_1, \ldots, D_m$ has the same cardinality. Use $D_i + \ell$ to denote the set

$$\{d + \ell \pmod{v} \mid d \in D_i\},$$

performing the modular arithmetic so as to ensure that $D_i + \ell \subseteq \{1, \ldots, v\}$. Then the sets

$$\{D_i + \ell \mid 1 \leq i \leq m, 0 \leq \ell \leq v - 1\}$$

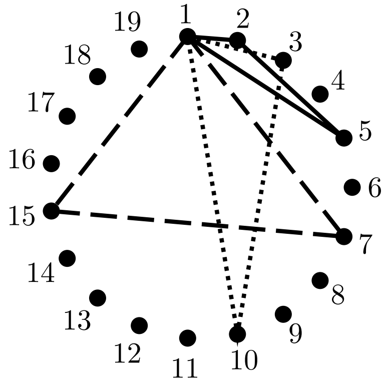
form a BIBD$(v, |D_1|, 1)$.

In the above example, taking the 57 sets $\{1, 2, 5\} + \ell$, $\{1, 3, 10\} + \ell$, and $\{1, 7, 15\} + \ell$, where $0 \leq \ell \leq 18$, gives a BIBD$(19, 3, 1)$.

Let's go over this construction again, thinking about the graph version of the problem. For simplicity, we'll look only at the special case $\lambda = 1$. So our object is to colour the edges of the complete graph K_v so as to ensure that every colour class is a K_k. If we draw the vertices of the graph in a circle, and think of the *length* of an edge as being one more than the number of vertices between its endvertices as you travel around the circle in whichever direction is shorter, then for every possible length between 1 and $(v-1)/2$, K_v has v edges of that length. (This is where the trouble arises if v is even: there are only $v/2$ edges of length $v/2$.) Furthermore, if we rotate any edge by one step around the graph (i.e. move both of its endpoints one step in the same direction) repeatedly, after v such rotations we will have moved the edge onto every other edge of that length.

These ideas demonstrate that if we can come up with a set of K_ks, such that every edge length appears in exactly one of the K_ks, then by taking each one of these as well as every possible rotation of each one of these, as a colour class, we find our desired edge-colouring of K_v.

A picture is worth a thousand words. The example above is equivalent to edge-colouring K_{19} so that every colour class forms a K_3, since $v = 19$ and $k = 3$. The edge lengths in K_{19} are $\{1, \ldots, 9\}$. We will show three K_3s, such that every edge length from $\{1, \ldots, 9\}$ appears in exactly one of them. By rotating each of them, giving each rotation a new colour, we obtain 57 K_3s that use every edge of K_{19} exactly once. We've labeled the vertices 1 through 19 to make the edge lengths easier to work out. This textbook is printed in black-and-white, so, instead of drawing actual colours on the edges, we will draw solid edges for blue, dotted edges for red, and dashed edges for green.



The solid (or blue) triangle has edges of lengths 1, 3, and 4; the dotted (or red) triangle has edges of lengths 2, 7, and 9; and the dashed (or green) triangle has edges of lengths 6, 8, and 5.

A design created using this method is called a *cyclic design*, since a small number of "starter blocks" are being rotated cyclically (in the graph) to find the remaining blocks of the design.

Notice that for a cyclic design to exist, since each set in the difference collection leads to v blocks in the final design, b must be a multiple of v.

Although these methods can successfully create designs with many different sets of parameters, they are not nearly enough to allow us to determine the parameters for which BIBDs exist. We noted previously that the necessary conditions given in Theorem 17.11 are not sufficient to guarantee the existence of a BIBD with a particular set of parameters. However, there is a very powerful result along these lines, known as Wilson's Theorem. It tells us that if we fix k, there are only finitely many values for v that satisfy the necessary conditions but for which no BIBD$(v, k, 1)$ exists. Then by Method 1 (repeating blocks), if a BIBD$(v, k, 1)$ exists, then so does a BIBD(v, k, λ) for any λ. Here is a formal statement of Wilson's Theorem.

THEOREM 17.19. Wilson's Theorem *Given k, there is an integer $v(k)$ such that for every $v > v(k)$ that satisfies the three conditions:*

- *$v \in \mathbb{Z}$;*

- *$v(v-1)/[k(k-1)] \in \mathbb{Z}$; and*
- *$(v-1)/(k-1) \in \mathbb{Z}$,*

a BIBD$(v, k, 1)$ exists.

We will not give a proof of this theorem.

EXERCISES 17.20.

1) Prove that the complement of a BIBD is indeed a design, and that it has the parameters we claimed in Proposition 17.15.
[*Hint:* Use inclusion-exclusion to determine how many blocks of the original design contain neither point from an arbitrary pair.]

2) Find the complement of the BIBD$(8, 4, 3)$ given by $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and

$$\mathcal{B} = \left\{\begin{matrix} \{1,2,3,4\}, & \{5,6,7,8\}, & \{1,2,5,6\}, & \{1,2,7,8\}, & \{3,4,5,6\}, & \{3,4,7,8\}, & \{2,4,6,8\}, \\ \{1,3,5,7\}, & \{1,3,6,8\}, & \{2,4,5,7\}, & \{1,4,5,8\}, & \{1,4,6,7\}, & \{2,3,5,8\}, & \{2,3,6,7\} \end{matrix}\right\}.$$

3) By adding two more sets to the sets $\{1, 3, 7\}$ and $\{1, 6, 13\}$, you can create a difference collection for 25 in which each of the sets has 3 elements, and thus a cyclic BIBD$(25, 3, 1)$. Find two sets to add.

4) Use a difference set to construct a cyclic $(11, 11, 5, 5, 2)$ design.

5) Show that the collection $\mathcal{C} = \big\{\{0, 1, 3\}, \{0, 4, 5\}, \{0, 4, 7\}, \{0, 5, 7\}\big\}$ is a difference collection for 13. Construct the design and give its parameters.

6) Determine whether the given set D is a difference set for the given value of n.
If it is a difference set, find the parameters of the resulting cyclic BIBD.
(a) $D = \{1, 2, 4, 10\}$ for $n = 13$.
(b) $D = \{2, 4, 5, 6, 10\}$ for $n = 21$.

7) Prove that in any cyclic design, there exists an integer c such that $b = cv$, $ck(k-1) = \lambda(v-1)$, and $r = ck$. What is the significance of c in terms of the design?

8) Explain why a BIBD with $v = 6$, $b = 10$, $k = 3$, $r = 5$, and $\lambda = 2$ cannot be cyclic.

9) Does the condition you proved in Problem 7 show that a BIBD with $v = 61$, $b = 305$, $k = 4$, $r = 20$, and $\lambda = 1$ cannot be cyclic?

17C. Fisher's Inequality

There is one more important inequality that is not at all obvious, but is necessary for the existence of a BIBD(v, k, λ). This is known as Fisher's Inequality, since it was proven by Fisher. The proof we will give is somewhat longer than the standard proof. This is because the standard proof uses linear algebra, which is not required background for this course.

THEOREM 17.21. Fisher's Inequality *For any BIBD(v, k, λ), we must have $b \geq v$.*

Before proving this fact, let's observe the consequences in terms of the usual parameters: v, k, and λ. We know from Equation 17.9 that

$$b = \frac{\lambda v(v-1)}{k(k-1)},$$

so $b \geq v$ implies

$$\frac{\lambda v(v-1)}{k(k-1)} \geq v.$$

Since v is the number of points of a design, it must be positive, so dividing through by v does not reverse the inequality. Thus,

$$\frac{\lambda(v-1)}{k(k-1)} \geq 1.$$

Since k is the number of points in each block, both k and $k-1$ must be positive (we are ignoring the trivial case $k=1$), so multiplying through by $k(k-1)$ does not reverse the inequality. Thus,

$$\lambda(v-1) \geq k(k-1).$$

PROOF OF FISHER'S INEQUALITY. Suppose we have an arbitrary BIBD(v,k,λ). Let B be an arbitrary block of this design. For each value of i between 0 and k (inclusive), let n_i denote the number of blocks $B' \neq B$ such that $|B' \cap B| = i$. (When we say $B' \neq B$ we allow the blocks to be equal as sets if the block B is a repeated block of the design; we are only insisting that B' not be the exact same block of the design as B.)

The following equations involving n_i are consequences of easy combinatorial proofs, together with the definition of n_i:

$$\sum_{i=0}^{k} n_i = b-1, \tag{17.22}$$

because both sides of this equation count every block except B.

$$\sum_{i=0}^{k} in_i = k(r-1), \tag{17.23}$$

because both sides of this equation count the number of times elements of B appear in some other block of the design.

$$\sum_{i=2}^{k} i(i-1)n_i = k(k-1)(\lambda-1),$$

because both sides of this equation count the number of times all of the ordered pairs of elements from B appear together in some other block of the design. Note that when $i=0$ or $i=1$, we have $i(i-1)n_i = 0$, so in fact

$$\sum_{i=0}^{k} i(i-1)n_i = \sum_{i=2}^{k} i(i-1)n_i = k(k-1)(\lambda-1). \tag{17.24}$$

Adding Equations 17.23 and 17.24 gives

$$\sum_{i=0}^{k} i^2 n_i = k(k-1)(\lambda-1) + k(r-1). \tag{17.25}$$

Now comes the part of the proof where something mysterious happens, and for reasons that are not at all apparent, the result we want will emerge. To fully understand a proof like this one requires deeper mathematics, but even seeing a proof is useful to convince ourselves that the result is true.

Take the polynomial in x given by

$$\sum_{i=0}^{k}(x-i)^2 n_i = \sum_{i=0}^{k}(x^2-2xi+i^2)n_i = x^2\sum_{i=0}^{k} n_i - 2x\sum_{i=0}^{k} in_i + \sum_{i=0}^{k} i^2 n_i.$$

Using Equations 17.22, 17.23, and 17.25, we see that this is equal to

$$x^2(b-1) - 2xk(r-1) + k(k-1)(\lambda-1) + k(r-1).$$

Notice that the format in which this polynomial started was a sum of squares times non-negative integers, so its value must be non-negative for any $x \in \mathbb{R}$.

Using the quadratic formula, $ax^2 + b'x + c = 0$ has roots at

$$\frac{-b' \pm \sqrt{(b')^2 - 4ac}}{2a}.$$

If a quadratic polynomial has two real roots, then there is a region in which its values are negative. Since this polynomial is non-negative for every $x \in \mathbb{R}$, it can have at most one real root, so $(b')^2 - 4ac \leq 0$. Substituting the actual values from our polynomial, this means that

$$(-2k(r-1))^2 - 4(b-1)(k(k-1)(\lambda-1) + k(r-1)) \leq 0.$$

Hence,

$$k^2(r-1)^2 - k(b-1)((k-1)(\lambda-1) + r - 1) \leq 0.$$

Let's rewrite the b in terms of v, r, and k. By Theorem 17.7, we have $bk = vr$, so

$$k(b-1) = bk - k = vr - k.$$

Hence

$$k^2(r-1)^2 - (vr-k)((k-1)(\lambda-1) + r - 1) \leq 0.$$

Expand the second term slightly, and multiply both sides of the inequality by $v - 1$:

$$k^2(r-1)^2(v-1) - (vr-k)(k-1)(\lambda-1)(v-1) - (vr-k)(r-1)(v-1) \leq 0.$$

In the middle expression, we have $(\lambda - 1)(v - 1)$. By Theorem 17.7, we know that $\lambda = r(k-1)/(v-1)$, so

$$\lambda - 1 = \frac{r(k-1) - (v-1)}{v-1}.$$

Therefore,

$$(\lambda-1)(v-1) = r(k-1) - v + 1.$$

Thus, we have

$$k^2(r-1)^2(v-1) - (vr-k)(k-1)(rk - r - v + 1) - (vr-k)(r-1)(v-1) \leq 0.$$

The next step is a lot of work to do by hand. Fortunately there is good math software that can perform routine tasks like this quickly. If we expand this inequality fully, remarkably it has a nice factorisation:

$$r(k-r)(v-k)^2 \leq 0.$$

Now, $r > 0$ for any design, and $(v-k)^2$ is a square, so must be nonnegative. Therefore, this inequality forces $k - r \leq 0$, so $k \leq r$. Hence $r/k \geq 1$. Using Theorem 17.7, we have

$$b = vr/k \geq v,$$

as desired. □

Notice that if k is fixed, then only finitely many values of v do not meet Fisher's Inequality, so satisfying this inequality did not need to be added as a condition to Wilson's Theorem.

EXERCISES 17.26.

1) Find values for v, k and λ that satisfy Theorem 17.11 but do not satisfy Fisher's Inequality. What can you say about the existence of a design with these parameters?
2) Suppose that $\lambda = 1$ and $k = 20$. How big must v be to satisfy Fisher's Inequality? What is the smallest value for v that satisfies all of the necessary conditions?
3) Suppose that $\lambda = 2$ and $k = 20$. How big must v be to satisfy Fisher's Inequality? What is the smallest value for v that satisfies all of the necessary conditions?
4) Explain how you know there does not exist a BIBD with $v = 46$, $b = 23$, and $k = 10$.

5) Explain how you know there does not exist a BIBD with $v = 8$, $b = 10$, $k = 4$, and $r = 5$.

6) If $\mathcal{B}$ is a BIBD with $v = 22$, then what can you say about the value of b?

SUMMARY:

- equivalence between designs and (multi)graph colouring/decomposition problem
- necessary conditions for a BIBD
- construction methods for designs
- Wilson's Theorem
- Fisher's Inequality
- Important definitions:
  - design
  - blocks
  - balanced, regular, uniform
  - BIBD
  - complementary design
  - difference collection
- Notation:
  - b, v, r, k, λ

Chapter 18

More designs

18A. Steiner and Kirkman triple systems

In 1844, W.S.B. Woolhouse, editor of the *Ladies and Gentleman's Diary*, posed that publication's annual prize problem:

> Determine the number of combinations that can be made of n symbols, p symbols in each, with this limitation, that no combination of q symbols which may appear in any one of them shall be repeated in any other.

If we take $q = 2$ then this is essentially a design with $k = p$ and $v = n$, although it need not be balanced; some pairs might appear once while other pairs do not appear. Although some responses were printed in 1845, they were not satisfactory, and in 1846 by Woolhouse repeated the question for the special case $q = 2$ and $p = 3$.

In 1847, Rev. Thomas Kirkman (previously mentioned in Chapter 13) found a complete solution to this problem in the case where the design is balanced (with $\lambda = 1$), and made some progress towards solving the complete problem. In our terminology, his solution completely determined the values of v for which a BIBD$(v, 3, 1)$ exists.

Although Steiner did not study triple systems in 1853, he came up with Kirkman's result independently, and his work was more broadly disseminated in mathematical circles, so these structures still carry his name. Despite this, as we shall see in the next section, there is a related problem that has been named after Kirkman.

DEFINITION 18.1. A **triple system** is a (regular) balanced design in which every block has cardinality 3; that is, a BIBD$(v, 3, \lambda)$.

A **Steiner triple system** is a triple system with $\lambda = 1$.

EXAMPLE 18.2. The cyclic BIBD$(19, 3, 1)$ given in Example 17.18 is a Steiner triple system. So is the design on 7 points given by

$$\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}.$$

NOTATION 18.3. Since the only variable in a Steiner triple system is v, for such a system on v points we use the notation STS(v).

Triple systems might seem like a very special case of designs, and it would be reasonable to wonder why we have chosen to single these out for special study and attention. The answer is that triple systems can be thought of as the smallest interesting examples of designs, since (as noted previously) if $k = 1$ there are no pairs in any block and the design is trivial; and if $k = 2$ then the blocks are simply copies of every possible pair from the set V. So triple systems are a natural starting point when we are learning about designs: they include examples that are are not too big or complicated to understand, but are non-trivial.

If you are now convinced that triple systems are worth studying, you might still be wondering about Steiner triple systems in particular. We've seen that the method of repeating blocks allows us to construct a triple system for any λ if we first have a triple system with $\lambda = 1$, so Steiner triple systems will be the rarest kind of triple system, and are therefore of particular interest.

In the remainder of this section, we will prove Kirkman's result characterising the values of v for which an STS(v) exists. To do this, we will require two results about the existence of special kinds of Latin squares. There are many connections in combinatorics!

The special kinds of Latin squares we require will be *symmetric*: that is, the entry in row i and column j must equal the entry in row j, column i. We will also specify the entries on the *main diagonal*: the positions for which the row number and the column number are the same.

LEMMA 18.4. *For every odd n, there is a symmetric Latin square of order n with $1, 2, \dots, n$ appearing in that order down the main diagonal.*

PROOF. Make the entries of the first row

$$1, (n+3)/2, 2, (n+5)/2, 3, \dots, (n-1)/2, n, (n+1)/2.$$

For $i \geq 2$, the entries of row i will be the entries of row $i-1$ shifted one position to the left.

Clearly all of the entries in any row are distinct. Also, since it takes n shifts to the left to return to the starting point, all of the entries in any column must be distinct.

Since the entry in row a, column b moves to the entry in row $a+1$ column $b-1$ (mod n), the positions in which this entry appears will be precisely the positions (x, y) for which $x + y \equiv a + b \pmod{n}$. Since $i + j = j + i$, the entry in column i of row j will be the same as the entry in column j of row i. Thus, the Latin square is symmetric.

The same argument shows that the entry in row i and column i will be the entry in position $2i - 1 \pmod{n}$ of row 1. But this is precisely where i has been placed, so this entry will be i, as desired. □

EXAMPLE 18.5. When $n = 11$, here is the (symmetric) Latin square constructed in the proof of Lemma 18.4:

1	7	2	8	3	9	4	10	5	11	6
7	2	8	3	9	4	10	5	11	6	1
2	8	3	9	4	10	5	11	6	1	7
8	3	9	4	10	5	11	6	1	7	2
3	9	4	10	5	11	6	1	7	2	8
9	4	10	5	11	6	1	7	2	8	3
4	10	5	11	6	1	7	2	8	3	9
10	5	11	6	1	7	2	8	3	9	4
5	11	6	1	7	2	8	3	9	4	10
11	6	1	7	2	8	3	9	4	10	5
6	1	7	2	8	3	9	4	10	5	11

You can see that this construction will not work when n is even, since the values of some of the entries given in the formulas would not be integers. In fact, it is not possible to construct a symmetric Latin square of order n with the entries $1, \dots n$ down the main diagonal when n is even. Fortunately, it is possible to construct something similar that will achieve what we will require.

LEMMA 18.6. *For every even n, there is a symmetric Latin square of order n with the values $1, \dots, n/2, 1, \dots, n/2$ appearing in that order down the main diagonal.*

PROOF. Make the entries of the first row

$$1, (n+2)/2, 2, (n+4)/2, 3, \ldots, (n-2)/2, n.$$

For $i \geq 2$, the entries of row i will be the entries of row $i-1$ shifted one position to the left.

The same arguments as in the proof of Lemma 18.4 show that this is a symmetric Latin square. The entry in row i and column i will be the entry in position $2i-1 \pmod{n}$ of row 1. These are the entries $1, 2, \ldots, n/2$ and since position

$$2(n+2j)/2 - 1 \equiv 2j - 1 \pmod{n},$$

the entries in positions (j, j) and $((n+2j)/2, (n+2j)/2)$ will be the same, so each of these entries will be repeated in the same order. □

EXAMPLE 18.7. When $n = 10$, here is the (symmetric) Latin square constructed in the proof of Lemma 18.6:

1	6	2	7	3	8	4	9	5	10
6	2	7	3	8	4	9	5	10	1
2	7	3	8	4	9	5	10	1	6
7	3	8	4	9	5	10	1	6	2
3	8	4	9	5	10	1	6	2	7
8	4	9	5	10	1	6	2	7	3
4	9	5	10	1	6	2	7	3	8
9	5	10	1	6	2	7	3	8	4
5	10	1	6	2	7	3	8	4	9
10	1	6	2	7	3	8	4	9	5

We are now ready to characterise the values of v for which there is an STS(v).

THEOREM 18.8. *An STS(v) exists if and only if* $v \equiv 1, 3 \pmod{6}$.

PROOF. We prove the two implications separately.

(⇒) Suppose that an STS(v) exists. Then by Theorem 17.11, the values

$$\lambda\frac{v-1}{k-1} = \frac{v-1}{2} \quad \text{and} \quad \lambda\frac{v(v-1)}{k(k-1)} = \frac{v(v-1)}{6}$$

must be integers. The first of these conditions tells us that v must be odd, so must be 1, 3, or 5 (mod 6). If $v \equiv 5 \pmod{6}$, then $v = 6q+5$ for some q, so

$$v(v-1)/6 = (6q+5)(6q+4)/6.$$

Since neither $6q+5$ nor $6q+4$ is a multiple of 3, this will not be an integer. Thus, the second condition eliminates the possibility $v \equiv 5 \pmod{6}$. Therefore, $v \equiv 1, 3 \pmod{6}$.

(⇐) Suppose that $v \equiv 1, 3 \pmod{6}$. We give separate constructions of Steiner triple systems on v points, depending on the congruence class of v. We will use the graph theoretic approach to the problem, so our goal is to find colour classes for the edges of K_v such that each colour class consists of a K_3.

$\boldsymbol{v \equiv 3}$ **(mod 6)** Say $v = 6q+3$. Label the vertices of K_{6q+3} with

$$u_1, \ldots, u_{2q+1}; v_1, \ldots, v_{2q+1}; \text{ and } w_1, \ldots, w_{2q+1}.$$

By Lemma 18.4, there is a Latin square of order $2q+1$ in which for every $1 \leq i \leq 2q+1$, the entry i appears in position (i, i).

For $1 \leq i, j \leq 2q+1$ with $i \neq j$, if the entry in position (i, j) of this Latin square is ℓ, then use new colours to colour the edges that join the vertices in each of the following sets:

$$\{u_i, u_j, v_\ell\}; \{v_i, v_j, w_\ell\}; \text{ and } \{w_i, w_j, u_\ell\}.$$

Since the Latin square was symmetric, both position (i,j) and position (j,i) give rise to the same colour classes. Since we consider every pair $i \neq j$, every edge of the form u_iu_j, v_iv_j, or w_iw_j has been coloured (we must have $i \neq j$ for such an edge to exist). Since the square is Latin, every possible entry ℓ occurs somewhere in row i, so every edge of the form u_iv_ℓ, v_iw_ℓ, or w_iu_ℓ has been coloured, except that we did not look at the entry of the Latin square in the position (i,j), where $i = j$. We know that the entry in position (i,i) is i, so the edges of the form u_iv_i, v_iw_i, and w_iu_i are the only edges that have not yet been coloured.

For each $1 \leq i \leq 2q+1$, make the edges joining u_i, v_i, and w_i into one colour class.

Now all of the edges of K_{6q+3} have been coloured, and each colour class forms a K_3, so we have constructed a Steiner triple system.

$\boldsymbol{v \equiv 1 \pmod 6}$ Say $v = 6q+1$. Label the vertices of K_{6q+1} with

$$u_1, \ldots, u_{2q}; v_1, \ldots, v_{2q}; \text{ and } w_1, \ldots, w_{2q}; x.$$

By Lemma 18.6, there is a Latin square of order $2q$ in which for every $1 \leq i \leq q$, the entry i appears in position (i,i), and for every $q+1 \leq i \leq 2q$, $i-q$ appears in position (i,i).

For $1 \leq i,j \leq 2q$ with $i \neq j$, if the entry in position (i,j) of this Latin square is ℓ, then use new colours to colour the edges that join the vertices in each of the following sets:

$$\{u_i, u_j, v_\ell\}; \{v_i, v_j, w_\ell\}; \text{ and } \{w_i, w_j, u_\ell\}.$$

Since the Latin square was symmetric, both position (i,j) and position (j,i) give rise to the same colour classes. Since we consider every pair $i \neq j$, every edge of the form u_iu_j, v_iv_j, or w_iw_j has been coloured (we must have $i \neq j$ for such an edge to exist). Since the square is Latin, every possible entry ℓ occurs somewhere in row i, so every edge of the form u_iv_ℓ, v_iw_ℓ, or w_iu_ℓ has been coloured, except that we did not look at the entry of the Latin square in the position (i,j), where $i = j$. We know that the entry in position (i,i) is i (if $i \leq q$) or $i-q$ (if $i > q$), so the only edges that have not yet been coloured are the edges of the form u_iv_i, v_iw_i, and w_iu_i when $i \leq q$ and u_iv_{i-q}, v_iw_{i-q}, and w_iu_{i-q} when $i > q$, as well as every edge incident with x.

For each $1 \leq i \leq q$, make the edges joining u_i, v_i, and w_i into one colour class. Observe that amongst the remaining edges that are not incident with x, every vertex other than x is an endvertex of precisely one of the edges. For example, if $i \geq q$ then u_iv_{i-q} is one of these edges, while if $i < q$, $w_{i+q}u_i$ is one of these edges, so either way, u_i is an endvertex of precisely one of these edges. Therefore, if for every $q+1 \leq i \leq 2q$ we use new colours to colour the edges that join the vertices in each of the following sets:

$$\{u_i, v_{i-q}, x\}; \{v_i, w_{i-q}, x\}; \text{ and } \{w_i, u_{i-q}, x\},$$

every edge incident with x (as well as all of our other remaining edges) will have been coloured.

Now all of the edges of K_{6q+1} have been coloured, and each colour class forms a K_3, so we have constructed a Steiner triple system. □

EXAMPLE 18.9. We will use the method of Theorem 18.8 to construct an STS(15).

We have $15 = 6(2) + 3$, so $q = 2$. The points of our design will be u_i, v_i, and w_i for $1 \leq i \leq 2q+1 = 5$, and we will require a symmetric Latin square of order 5. Here is the square:

$$\begin{array}{ccccc}
1 & 4 & 2 & 5 & 3 \\
4 & 2 & 5 & 3 & 1 \\
2 & 5 & 3 & 1 & 4 \\
5 & 3 & 1 & 4 & 2 \\
3 & 1 & 4 & 2 & 5
\end{array}$$

Here are the blocks we form from this Latin square:

$$\begin{array}{llllll}
\{u_1,u_2,v_4\}, & \{v_1,v_2,w_4\}, & \{w_1,w_2,u_4\}, & \{u_1,u_3,v_2\}, & \{v_1,v_3,w_2\}, & \{w_1,w_3,u_2\}, \\
\{u_1,u_4,v_5\}, & \{v_1,v_4,w_5\}, & \{w_1,w_4,u_5\}, & \{u_1,u_5,v_3\}, & \{v_1,v_5,w_3\}, & \{w_1,w_5,u_3\}, \\
\{u_2,u_3,v_5\}, & \{v_2,v_3,w_5\}, & \{w_2,w_3,u_5\}, & \{u_2,u_4,v_3\}, & \{v_2,v_4,w_3\}, & \{w_2,w_4,u_3\}, \\
\{u_2,u_5,v_1\}, & \{v_2,v_5,w_1\}, & \{w_2,w_5,u_1\}, & \{u_3,u_4,v_1\}, & \{v_3,v_4,w_1\}, & \{w_3,w_4,u_1\}, \\
\{u_3,u_5,v_4\}, & \{v_3,v_5,w_4\}, & \{w_3,w_5,u_4\}, & \{u_4,u_5,v_2\}, & \{v_4,v_5,w_2\}, & \{w_4,w_5,u_2\},
\end{array}$$

$$\{u_1,v_1,w_1\},\{u_2,v_2,w_2\},\{u_3,v_3,w_3\},\{u_4,v_4,w_4\},\{u_5,v_5,w_5\}$$

After solving Woolhouse's problem, Kirkman noticed that his construction of an STS(15) had a very nice property. He challenged others to come up with this solution in the following problem that he published in the 1850 edition of the *Ladies and Gentleman's Diary*:

> Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast.

This has become known as Kirkman's Schoolgirl Problem.

Although this problem begins by requiring an STS(15), it has the additional requirement that it must be possible to partition the blocks of this design (the rows of young ladies) into seven groups (of five blocks each) so that every point (young lady) appears exactly once in each group. This extra requirement comes from the fact that each of the young ladies must walk out every day, and can only be in one row in any given day.

DEFINITION 18.10. A BIBD is a **resolvable design** if the blocks of the design can be partitioned into sets, each of which forms a partition of the point set of the BIBD.

A **Kirkman triple system** is a resolvable Steiner triple system.

Notice that since each block has 3 points in it, a Kirkman triple system is only possible if $v/3$ is an integer. Since a Kirkman triple system is also a Steiner triple system, this means that we must have $v \equiv 3 \pmod 6$.

There are seven non-isomorphic Kirkman triple systems of order 15.

Kirkman triple systems are also known to exist whenever $v \equiv 3 \pmod 6$.

THEOREM 18.11 (Chaudhury-Wilson, 1971). *There is a Kirkman triple system whenever* $v \equiv 3 \pmod 6$.

EXERCISES 18.12.

1) For $v = 37$, give the Latin square you would have to use in order to construct a Steiner triple system using the method described in the proof of Theorem 18.8.

2) For $v = 39$, give the Latin square you would have to use in order to construct a Steiner triple system using the method described in the proof of Theorem 18.8.

3) For $v = 19$, use the method described in the proof of Theorem 18.8 to construct a Steiner triple system.

4) Is the STS(15) constructed in Example 18.9 a Kirkman triple system? Explain your answer.
[*Hint:* Think of Pigeonhole-type arguments.]

5) Find all values of λ for which a triple system on six varieties exists. For each such value of λ, either give a design or explain how to construct it.
[*Hint:* Begin by showing that if such a design exists, its parameters are $(2r, 6, r, 3, 2r/5)$. Then determine what values r can take on. Finally use some results about how to construct designs.]

6) Construct an STS(13) design. Show your work.

7) Let $v = 21$.

(a) Write down the Latin square that you would use to construct a Steiner triple system (for this value of v) using the method described in the proof of Theorem 18.8.

(b) For the resulting Steiner triple system, which triples contain:

(i) both u_1 and u_3?

(ii) both v_2 and w_7?

(iii) both u_3 and w_4?

(iv) both v_5 and w_5?

(v) w_3?

8) Let $v = 27$.

(a) Write down the Latin square that you would use to construct a Steiner triple system (for this value of v) using the method described in the proof of Theorem 18.8.

(b) For the resulting Steiner triple system, which triples contain:

(i) both v_3 and u_8?

(ii) both u_4 and w_4?

(iii) both u_5 and w_4?

(iv) v_2?

(v) both v_2 and v_5?

18B. t-designs

In a BIBD, every *pair* appears together λ times. In the notation of Woolhouse's problem, $q = 2$. What about larger values of q? (We'll still only consider the case where every q-set appears an equal number of times λ, so the design must be balanced, but we will include the more general situation that $\lambda \geq 1$.)

DEFINITION 18.13. A **t-(v, k, λ) design** is a design on v points with blocks of cardinality k, such that every t-subset of V appears in exactly λ blocks.

So far, all we have looked at have been 2-designs.

THEOREM 18.14. *In a t-(v, k, λ) design,*

$$\binom{k-i}{t-i} \text{ is a divisor of } \lambda\binom{v-i}{t-i} \text{ for every } 0 \leq i \leq t-1.$$

PROOF. We first consider the special case where $i = 0$. Notice that in each of the b blocks, there are $\binom{k}{t}$ subsets of cardinality t that appear in that block. So in the entire design, $b\binom{k}{t}$ subsets of cardinality t appear.

There exist $\binom{v}{t}$ subsets of cardinality t from the v points of V, and each appears in λ blocks, so in the entire design, $\lambda\binom{v}{t}$ subsets of cardinality t appear.

Thus, $b\binom{k}{t} = \lambda\binom{v}{t}$.

Similarly, if we fix any set of i varieties, there are $\binom{v-i}{t-i}$ subsets of cardinality t that include these i varieties. Each such subset appears in λ blocks. However, for each of the blocks that contains these i elements (the number of these will be our quotient), we can complete our i-set to a set of cardinality t that lies within this block, in $\binom{k-i}{t-i}$ ways. Thus, we have counted any such block $\binom{k-i}{t-i}$ times in the preceding count. So $\binom{k-i}{t-i}$ must be a divisor of $\lambda\binom{v-i}{t-i}$, as claimed. □

EXAMPLE 18.15. Show that there is no $5-(16,7,1)$ design.

SOLUTION. We check the necessary conditions given in Theorem 18.14. Using the condition when $i=0$, we see that $b\binom{7}{5}=1\binom{16}{5}$, so $21b=4368$. Therefore $b=208$. This condition is satisfied.

When $i=1$ we have $\binom{k-i}{t-i}=\binom{6}{4}=15$, and $\lambda\binom{v-i}{t-i}=\binom{15}{4}=\frac{15\cdot14\cdot13\cdot12}{4\cdot3\cdot2}=15\cdot7\cdot13$, which is divisible by 15. This condition is satisfied.

When $i=2$ we have $\binom{k-i}{t-i}=\binom{5}{3}=10$, and $\lambda\binom{v-i}{t-i}=\binom{14}{3}=\frac{14\cdot13\cdot12}{3\cdot2}=14\cdot13\cdot2$, which is not divisible by 10 since it is not a multiple of 5. This condition fails. Thus, there is no $5-(16,7,1)$ design. □

Suppose we have a 3-$(10,4,1)$ design. By Theorem 18.14, it will have

$$b\binom{4}{3}=1\binom{10}{3},$$

so $4b=10\cdot9\cdot8/6=120$. Thus, $b=30$. Also, since $bk=vr$, we have $30\cdot4=10r$, so $r=12$.

EXAMPLE 18.16. Here is a 3-$(10,4,1)$ design.

$$\begin{array}{cccccc}
\{1,5,6,10\}, & \{1,2,8,9\}, & \{2,3,6,7\}, & \{3,4,9,10\}, & \{4,5,7,8\}, & \{1,3,4,7\}, \\
\{2,4,5,10\}, & \{1,3,5,8\}, & \{1,2,4,6\}, & \{2,3,5,9\}, & \{4,6,8,9\}, & \{1,7,9,10\}, \\
\{3,6,8,9\}, & \{5,6,7,9\}, & \{2,7,8,10\}, & \{1,2,3,10\}, & \{1,2,5,7\}, & \{1,4,5,9\}, \\
\{1,3,6,9\}, & \{1,6,7,8\}, & \{1,4,8,10\}, & \{2,3,4,8\}, & \{2,4,7,9\}, & \{2,5,6,8\}, \\
\{2,6,9,10\}, & \{3,4,5,6\}, & \{3,5,7,10\}, & \{3,7,8,9\}, & \{4,6,7,10\}, & \{5,8,9,10\}
\end{array}$$

Notice: For $t\geq 3$, a t-design is also a $(t-1)$-design. If every t-set appears in exactly λ blocks, then any $(t-1)$-set must appear in exactly

$$\lambda(v-t+1)/(k-t+1)$$

blocks. This is because if we fix a $(t-1)$-set, it can be made into a t-set by adding any one of the $v-t+1$ other elements of V. Each of these t-sets appears in λ of the blocks. However, some of these blocks are the same; in fact, we have counted each block containing this $(t-1)$-set once for every other element of the block (since every other element of the block forms a t-set when put together with the $(t-1)$-set). So every block that contains this $(t-1)$-set has been counted $k-(t-1)$ times. The result follows. (From the above formula we can see that $k-t+1$ is a divisor of $\lambda(v-t+1)$; this is exactly the condition that Theorem 18.14 gives when we take $i=t-1$.)

Therefore, since

$$1(10-3+1)/(4-3+1)=4,$$

the $3-(10,4,1)$ design that we gave above, is also a $2-(10,4,4)$ design. In more generality, a $t-(v,k,\lambda)$ design with $t>2$ is also a $(t-1)-(v,k,\lambda(v-t+1)/(k-t+1))$ design.

Steiner's name is also used in this more general context, and without the constraint on the block sizes.

DEFINITION 18.17. A **Steiner system** is a t-design with $\lambda=1$.

The 3-$(10,4,1)$ design above is a Steiner system.

Our ability to construct Steiner systems when $k>3$, or when $t>2$, except in trivial cases, is almost nonexistence. In fact, there are no known constructed Steiner systems with $t>5$, with the exception that taking every possible t-subset of a v-set is always a (trivial) $t-(v,t,1)$ design.

Despite this, in 2014 a remarkable theorem was proved by Peter Keevash, along similar lines to Wilson's Theorem, but applying to this more general context.

The necessary conditions given in Theorem 18.14 are not sufficient to guarantee the existence of a BIBD with a particular set of parameters. However, Keevash's Theorem tells us that if we fix k and t, there are only finitely many values for v that satisfy the necessary conditions but for which no $t-(v,k,1)$ design exists. His proof was probabilistic, so does not produce constructions for any designs. Here is a formal statement of Keevash's Theorem.

THEOREM 18.18. Keevash's Theorem *Given k and t, there is an integer $v(k,t)$ such that for every $v > v(k,t)$ that satisfies the conditions:*

- *$v \in \mathbb{Z}$; and*
- *for every $0 \le i \le t-1$,*

$$\binom{k-i}{t-i} \textit{ is a divisor of } \lambda\binom{v-i}{t-i}.$$

a $t-(v,k,1)$ design exists.

We will not give a proof of this theorem.

EXERCISES 18.19.

1) Substituting $t=2$ into the equations of Theorem 18.14 doesn't immediately look like either of the equations in Theorem 17.7. Use the equations of Theorem 17.7 to deduce that

$$\binom{k}{2} \text{ is a divisor of } \lambda\binom{v}{2}.$$

2) If $v=15$ and $\lambda=1$, what are all possible values of k and $t \ge 2$ for which t-designs might exist? Do not include any trivial $t-(v,t,1)$ design, so you may assume $v > k > t$.

3) Is it possible for a 3-$(16,6,1)$ design to exist? If so, how many blocks will it have? What will the value of r be?

4) Let $\mathcal{B}$ be the $(7,3,1)$-design. Define a new design D as follows, on the varieties $\{1,\ldots,8\}$. It has 14 blocks, of two types:

   (I) the blocks of $\mathcal{B}$ but with variety 8 added to each; and

   (II) the blocks of the complementary design to $\mathcal{B}$.

   Prove that this is a Steiner system with $t=3$, $k=4$ and $v=8$. Use the structure of $\mathcal{B}$ and its complement to show that $\lambda=1$; do not check all $\binom{8}{3}$ possible 3-subsets of $\{1,\ldots,8\}$.

5) Define a design as follows. Label the edges of the complete graph K_6; these will be the varieties of the design. The blocks are of two types:

   - (I) any set of three edges from K_6 that can be properly coloured with the same colour; and
   - (II) any set of three edges that form a triangle in K_6.

   Determine the parameters of this t-design (including the highest value of t for which this is a t-design, and justifying each value you determine), and show that this is a Steiner system.

6) Might a $3-(20,5,8)$ design exist according to the necessary conditions we have determined (Theorem 18.14)? State the formulas that must be satisfied and show your work.

18C. Affine planes

You are probably familiar with at least some of Euclid's axioms of geometry. The following are amongst Euclid's axioms (we have not used the same terms Euclid used in his *Elements*, but commonly-used statements that are equivalent to Euclid's):

Key Euclidean Axioms

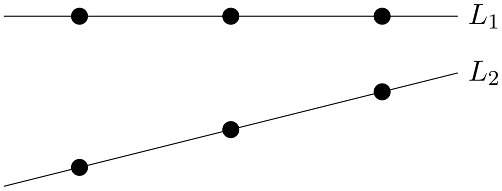
- Any two points determine (and so lie together on) a unique line.
- (Parallel postulate) For any line L, and any point p that does not lie on the line L, there is a unique line L' through p that is parallel to L; that is, L and L' have no points in common.

If you haven't taken geometry classes in university, you may not know that we can apply these axioms to finite sets of points, and discover structures that we call *finite Euclidean geometries*, or more commonly, *affine planes*. To avoid some trivial situations, we also require that the structure has at least three points, and that not all of the points lie on a single line.

The following definition probably seems obvious.

DEFINITION 18.20. We say that two lines are **parallel** if no point lies on both lines.

We've made special note of this definition because in the finite case, "parallel" lines might be drawn in such a way that they don't look parallel according to our usual understanding of the term. Since each line has only a finite number of points on it, two lines L_1 and L_2 are parallel as long as none of the points on L_1 also lies on L_2, even if in a particular drawing in appears that these lines will meet if we extend them. In the figure below, lines L_1 and L_2 have three points each, and the lines are parallel.



DEFINITION 18.21. A (finite) **affine plane** consists of a (finite) set of points, a (finite) set of lines, and an incidence relation between the points and the lines. The incidence relation must satisfy these Euclidean axioms:

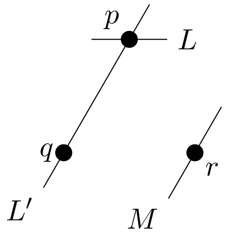
- Any two points lie together on a unique line.
- For any line L, and any point p that does not lie on the line L, there is a unique line L' that passes through p and is disjoint from L (that is, it is parallel to L).
- There are at least three points that are not all on the same line.

For the purposes of this book, we will only consider finite affine planes, so assume from now on that the set of points is finite. It is not very obvious, but the parallel postulate (together with the final axiom) ensure that it is not possible to have a line that doesn't contain any points, so the set of lines will also be finite.

There is a very nice bijective argument that can be used to show that the number of points on any two lines is equal. Before presenting this, we show that there cannot be a line that contains only one point.

PROPOSITION 18.22. *In a finite affine plane, no line contains only one point.*

PROOF. The following diagram may be a helpful visual aid as you read through the proof below.

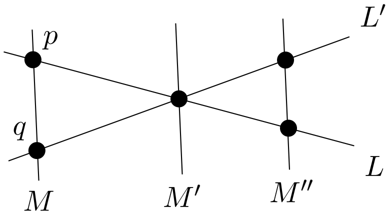


Towards a contradiction, suppose that there were a line L that contained only a single point, p. By the final axiom, there are at least two other points in the finite affine plane, q and r, that do not both lie on a line with p. By the first axiom, there is a line L' that contains both p and q (but by our choice of q and r, L' does not contain r). Now by the parallel postulate, there is a line M through r that is parallel to L'. Furthermore, there is a unique line through p that is parallel to M. But we know that M is parallel to L'; in addition, M does not contain p, so it is also parallel to L; this is a contradiction. □

We can now show that every line contains the same number of points.

PROPOSITION 18.23. *In a finite affine plane, if one line contains exactly n points, then every line contains exactly n points.*

PROOF. Again, we begin with a diagram that may be a helpful visual aid to understanding this proof.



Let L be a line that contains exactly n points, and let L' be any other line of the finite affine plane. By Proposition 18.22, we know that $n > 1$, and that L' also contains at least two points (we observed above that no line can be empty of points). Since any two points lie together on a unique line, if L and L' meet, they meet in a single point, so there is a point p of L that is not in L', and a point q of L' that is not in L. By the first axiom, there is a line M that contains the points p and q.

We define a map ψ from points of L to points of L' as follows. Let $\psi(p) = q$. For any other point p' of L (with $p' \neq p$), by the parallel postulate there is a unique line M' through p' that is parallel to M. Since M passes through q and is parallel to M', it is the unique line with this property, so in particular, L' cannot be parallel to M'. Therefore, M' has a unique point of intersection, say q', with L'. Define $\psi(p') = q'$. Since M' and q' were uniquely determined, the map ψ is well-defined (that is, there is no ambiguity about which point of L' is found to be $\psi(p')$).

We claim that ψ is a bijection between the points of L and the points of L'; proving this will complete the proof. We first show that ψ is one-to-one. Suppose that $\psi(p_1) = q_1$, $\psi(p_2) = q_2$, and q_1 and q_2 are actually the same point of L'. Then by the definition of ψ, q_1 is on some line M_1 that is parallel to M, and contains p_1, while q_2 is on some line M_2 that is parallel to M, and contains p_2. Since $q_1 = q_2$, the parallel postulate tells us that we must have $M_1 = M_2$. This line can only meet L in a single point, so we must have $p_1 = p_2$. Thus, ψ is one-to-one.

To show that ψ is onto, let q'' be any point of L' with $q'' \neq q$ (we already know that q has a pre-image, p). By the parallel postulate, there is a unique line M'' through q'' that is parallel to M. Since M is the unique line through p that is parallel to M'', we see that L is not parallel to M'', so L must meet M'' at some point that we will call p''. Now by the definition of ψ, we have $\psi(p'') = q''$. Thus, q'' has a pre-image, so ψ is onto. □

We refer to the number of points on each line of a finite affine plane as the *order* of the plane. We can now figure out how many points are in a finite affine plane of order n.

PROPOSITION 18.24. *A finite affine plane of order n has n^2 points.*

PROOF. Since the plane has at least three points, not all of which lie on the same line, it has at least two lines L and L' that intersect at a point q but are not equal. We know that each of these lines contains n points. By the parallel postulate, for each of the $n-1$ points on L' that is not on L, there is a line through that point that is parallel to L. Now, L and these $n-1$ lines that are parallel to L each contain n points, and since they are all parallel (it is an exercise, see below, to prove that if M is parallel to L and N is parallel to L, then N is parallel to M), these points are all distinct. Therefore the plane has at least n^2 points.

Consider any point p that is not on L. By the parallel postulate, there must be a line P through p that is parallel to L. Now, L is the unique line through q that is parallel to P, so in particular, L' is not parallel to P. Therefore, L' and P have a point of intersection, which is one of the $n-1$ points of L' that is not on L. So P was one of the $n-1$ lines that we found in our first paragraph, meaning that p is one of the n^2 points that we found there. Thus, the plane has exactly n^2 points. □

You might be wondering by now why we are spending so much time looking at affine planes, when they are a geometric structure. Despite the fact that they come from geometry, finite affine planes can be thought of as a special kind of design.

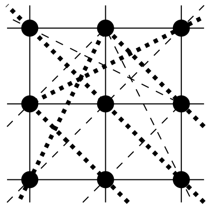
Think of the points of a finite affine plane as points of a design, and the lines as blocks, with a point being in a block if it is incident with (on) the corresponding line. The first axiom for the incidence relation guarantees that every pair of points appear together in exactly one block, so our design has $\lambda = 1$. By Proposition 18.23, we see that an affine plane of order n is uniform, with $k = n$. By Proposition 18.24, an affine plane of order n has $v = n^2$. Although we have not included a proof of this, it can also be shown that this design is regular, so it is in fact a BIBD$(n^2, n, 1)$.

Using

$$b\binom{k}{t} = \lambda\binom{v}{t}$$

from Theorem 18.14, we see that in a finite affine plane of order n looked at as a design, we have $b\binom{n}{2} = \binom{n^2}{2}$, so $bn(n-1) = n^2(n^2-1)$. Hence $b = n(n+1)$. In other words, a finite affine plane of order n has $n(n+1)$ lines.

EXAMPLE 18.25. A finite affine plane of order 3 has $3^2 = 9$ points. Each line has 3 points, and there are $3(4) = 12$ lines. Since each line has three points, every line lies in a parallel class consisting of three mutually parallel lines, so there are four such parallel classes. We can choose two of the parallel classes of lines to be "horizontal" and "vertical" lines. The other two classes will be the two types of diagonal lines. We can't draw all of these as straight lines, so we have drawn one parallel class of lines as sets of three points joined by dashes, and the other as sets of three points joined by dots.



The dashes and dots that join sets of points that aren't in a straight line may not provide a very clear image of what's going on; it is probably clearer to think of the diagonal lines as "wrapping around" when they go off the bottom, top, or either side of the image, and reappearing on the opposite side.

There is a nice connection between affine planes and mutually orthogonal Latin squares.

THEOREM 18.26. *There is an affine plane of order $n > 1$ if and only if there are $n-1$ mutually orthogonal Latin squares of order n.*

PROOF. ($\Rightarrow$) An affine plane of order n has $n+1$ classes of parallel lines (each class containing n lines). Consider two of these sets as the horizontal lines and the vertical lines: $H_1, \ldots, H_n$ and $V_1, \ldots, V_n$. Label a point as (i, j) if it lies at the intersection of V_i and H_j. Since each of the n^2 points lies on a vertical line and on a horizontal line, and since every pair of points lie together on only one line, this is actually a bijection between $\{1, \ldots, n\} \times \{1, \ldots, n\}$ and the points of the affine plane; that is, this provides n^2 coordinates that uniquely determine the n^2 points of the plane.

Consider any one of the remaining parallel classes of n lines, $L_1, \ldots, L_n$. Observe that every point of the affine plane lies on precisely one of these lines. Create a Latin square from this parallel class by placing k in position (i, j) of the Latin square if and only if the point (i, j) of the affine plane lies on line L_k. Since every line of $L_1, \ldots, L_n$ meets every line of $H_1, \ldots, H_n$ exactly once (by the axioms of an affine plane), each entry will appear exactly once in each row. Similarly, since every line of $L_1, \ldots, L_n$ meets every line of $V_1, \ldots, V_n$ exactly once (by the axioms of an affine plane), each entry will appear exactly once in each column. So we have indeed created a Latin square.

We will now show that the $n-1$ Latin squares created by this method (using the $n-1$ parallel classes of lines that remain after excluding the ones we have designated as horizontal and vertical lines) are mutually orthogonal. We'll do this by considering two arbitrary Latin squares, L (coming from the lines $L_1, \ldots, L_n$) and M (coming from the lines $M_1, \ldots, M_n$). In position (i, j), the entry of L being i' means that line $L_{i'}$ passes through the point (i, j) (which is the intersection of lines V_i and H_j). Similarly, this entry of M being j' means that line $M_{j'}$ passes through the point (i, j) (which is the intersection of lines V_i and H_j). Since the lines $L_{i'}$ and $M_{j'}$ have a unique point of intersection, there cannot be any other positions in which the entry of L is i' while the entry of M is j'. Thus, each ordered pair $(i', j') \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ must appear in exactly one position as the entries of L and M (in that order), and hence L and M are orthogonal. Since they were arbitrary, we have $n-1$ mutually orthogonal Latin squares.

($\Leftarrow$) The converse of this proof uses the same idea, in the opposite direction. Given $n-1$ mutually orthogonal n by n Latin squares, take the n^2 coordinate positions to be the points of our affine plane. Define two parallel classes of lines (each containing n lines) to be the points whose first coordinate is equal (so all of the points with first coordinate 1 form one line, and all of the points with first coordinate 2 form a second line, etc.), and the points whose second coordinate is equal. Each of the $n-1$ Latin squares determines an additional parallel class of n lines: namely, each line consists of the points for which the entry of the Latin square has some fixed value. Since $n > 1$, there are clearly at least three points that are not all on the same line. We leave it as an exercise to prove that any two points lie together in a unique line, and that the parallel postulate is satisfied. □

EXAMPLE 18.27. Use the formula from the proof of Theorem 16.10 to construct 6 MOLS of order 7. Use the construction given in the proof of Theorem 18.26 to construct an affine plane of order 7 from your squares.

SOLUTION. The squares will be:

$$\begin{array}{ccccccc@{\qquad}ccccccc}
0&1&2&3&4&5&6&0&1&2&3&4&5&6\\
1&2&3&4&5&6&0&2&3&4&5&6&0&1\\
2&3&4&5&6&0&1&4&5&6&0&1&2&3\\
3&4&5&6&0&1&2&6&0&1&2&3&4&5\\
4&5&6&0&1&2&3&1&2&3&4&5&6&0\\
5&6&0&1&2&3&4&3&4&5&6&0&1&2\\
6&0&1&2&3&4&5&6&0&1&2&3&4&5\\
\hline
0&1&2&3&4&5&6&0&1&2&3&4&5&6\\
3&4&5&6&0&1&2&4&5&6&0&1&2&3\\
6&0&1&2&3&4&5&1&2&3&4&5&6&0\\
2&3&4&5&6&0&1&5&6&0&1&2&3&4\\
5&6&0&1&2&3&4&2&3&4&5&6&0&1\\
1&2&3&4&5&6&0&6&0&1&2&3&4&5\\
4&5&6&0&1&2&3&3&4&5&6&0&1&2\\
\hline
0&1&2&3&4&5&6&0&1&2&3&4&5&6\\
5&6&0&1&2&3&4&6&0&1&2&3&4&5\\
3&4&5&6&0&1&2&5&6&0&1&2&3&4\\
1&2&3&4&5&6&0&4&5&6&0&1&2&3\\
6&0&1&2&3&4&5&3&4&5&6&0&1&2\\
4&5&6&0&1&2&3&2&3&4&5&6&0&1\\
2&3&4&5&6&0&1&1&2&3&4&5&6&0
\end{array}$$

The affine plane will have $7^2 = 49$ points, and we will denote these as ordered pairs (a, b), where $a, b \in \{1, \ldots, 7\}$ and consider them to represent the 49 positions in a 7 by 7 Latin square. There will be $7(8) = 56$ lines, in 8 parallel classes of seven lines each. Although we could draw the affine plane, you've already seen from the affine plane of order 3 that a black-and-white image all of which is pre-drawn can be more confusing than helpful, so instead we will list each of the 56 lines as a set of 7 points.

The first parallel class will represent the horizontal rows:

$$\begin{array}{ll}
\{(1,1),(2,1),(3,1),(4,1),(5,1),(6,1),(7,1)\}, & \{(1,2),(2,2),(3,2),(4,2),(5,2),(6,2),(7,2)\},\\
\{(1,3),(2,3),(3,3),(4,3),(5,3),(6,3),(7,3)\}, & \{(1,4),(2,4),(3,4),(4,4),(5,4),(6,4),(7,4)\},\\
\{(1,5),(2,5),(3,5),(4,5),(5,5),(6,5),(7,5)\}, & \{(1,6),(2,6),(3,6),(4,6),(5,6),(6,6),(7,6)\},\\
\{(1,7),(2,7),(3,7),(4,7),(5,7),(6,7),(7,7)\} &
\end{array}$$

and similarly the second parallel class will represent the vertical rows:

$$\begin{array}{ll}
\{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(1,7)\}, & \{(2,1),(2,2),(2,3),(2,4),(2,5),(2,6),(2,7)\},\\
\{(3,1),(3,2),(3,3),(3,4),(3,5),(3,6),(3,7)\}, & \{(4,1),(4,2),(4,3),(4,4),(4,5),(4,6),(4,7)\},\\
\{(5,1),(5,2),(5,3),(5,4),(5,5),(5,6),(5,7)\}, & \{(6,1),(6,2),(6,3),(6,4),(6,5),(6,6),(6,7)\},\\
\{(7,1),(7,2),(7,3),(7,4),(7,5),(7,6),(7,7)\}. &
\end{array}$$

The remaining six parallel classes will each represent one of the Latin squares. In the next parallel class, the first line consists of all of the points where the entry of the first Latin square is 0; the second consists of all the points where the entry is 1, and so on.

$$\begin{array}{ll}
\{(1,1),(7,2),(6,3),(5,4),(4,5),(3,6),(2,7)\}, & \{(2,1),(1,2),(7,3),(6,4),(5,5),(4,6),(3,7)\},\\
\{(3,1),(2,2),(1,3),(7,4),(6,5),(5,6),(4,7)\}, & \{(4,1),(3,2),(2,3),(1,4),(7,5),(6,6),(5,7)\},\\
\{(5,1),(4,2),(3,3),(2,4),(1,5),(7,6),(6,7)\}, & \{(6,1),(5,2),(4,3),(3,4),(2,5),(1,6),(7,7)\},\\
\{(7,1),(6,2),(5,3),(4,4),(3,5),(2,6),(1,7)\}. &
\end{array}$$

The next parallel class comes from the second Latin square (reading across, so the second square is the second one in the first line):

$$\begin{array}{ll}
\{(1,1),(6,2),(4,3),(2,4),(7,5),(5,6),(3,7)\}, & \{(2,1),(7,2),(5,3),(3,4),(1,5),(6,6),(4,7)\},\\
\{(3,1),(1,2),(6,3),(4,4),(2,5),(7,6),(5,7)\}, & \{(4,1),(2,2),(7,3),(5,4),(3,5),(1,6),(6,7)\},\\
\{(5,1),(3,2),(1,3),(6,4),(4,5),(2,6),(7,7)\}, & \{(6,1),(4,2),(2,3),(7,4),(5,5),(3,6),(1,7)\},\\
\{(7,1),(5,2),(3,3),(1,4),(6,5),(4,6),(2,7)\}. &
\end{array}$$

From the third Latin square:

$$\begin{array}{ll}
\{(1,1),(5,2),(2,3),(6,4),(3,5),(7,6),(4,7)\}, & \{(2,1),(6,2),(3,3),(7,4),(4,5),(1,6),(5,7)\},\\
\{(3,1),(7,2),(4,3),(1,4),(5,5),(2,6),(6,7)\}, & \{(4,1),(1,2),(5,3),(2,4),(6,5),(3,6),(7,7)\},\\
\{(5,1),(2,2),(6,3),(3,4),(7,5),(4,6),(1,7)\}, & \{(6,1),(3,2),(7,3),(4,4),(1,5),(5,6),(2,7)\},\\
\{(7,1),(4,2),(1,3),(5,4),(2,5),(6,6),(3,7)\}. &
\end{array}$$

From the fourth Latin square:

$$\begin{array}{ll}
\{(1,1),(4,2),(7,3),(3,4),(6,5),(2,6),(5,7)\}, & \{(2,1),(5,2),(1,3),(4,4),(7,5),(3,6),(6,7)\},\\
\{(3,1),(6,2),(2,3),(5,4),(1,5),(4,6),(7,7)\}, & \{(4,1),(7,2),(3,3),(6,4),(2,5),(5,6),(1,7)\},\\
\{(5,1),(1,2),(4,3),(7,4),(3,5),(6,6),(2,7)\}, & \{(6,1),(2,2),(5,3),(1,4),(4,5),(7,6),(3,7)\},\\
\{(7,1),(3,2),(6,3),(2,4),(5,5),(1,6),(4,7)\}. &
\end{array}$$

From the fifth Latin square:

$$\begin{array}{ll}
\{(1,1),(3,2),(5,3),(7,4),(2,5),(4,6),(6,7)\}, & \{(2,1),(4,2),(6,3),(1,4),(3,5),(5,6),(7,7)\},\\
\{(3,1),(5,2),(7,3),(2,4),(4,5),(6,6),(1,7)\}, & \{(4,1),(6,2),(1,3),(3,4),(5,5),(7,6),(2,7)\},\\
\{(5,1),(7,2),(2,3),(4,4),(6,5),(1,6),(3,7)\}, & \{(6,1),(1,2),(3,3),(5,4),(7,5),(2,6),(4,7)\},\\
\{(7,1),(2,2),(4,3),(6,4),(1,5),(3,6),(5,7)\}. &
\end{array}$$

And finally,

$$\begin{array}{ll}
\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7)\}, & \{(2,1),(3,2),(4,3),(5,4),(6,5),(7,6),(1,7)\},\\
\{(3,1),(4,2),(5,3),(6,4),(7,5),(1,6),(2,7)\}, & \{(4,1),(5,2),(6,3),(7,4),(1,5),(2,6),(3,7)\},\\
\{(5,1),(6,2),(7,3),(1,4),(2,5),(3,6),(4,7)\}, & \{(6,1),(7,2),(1,3),(2,4),(3,5),(4,6),(5,7)\},\\
\{(7,1),(1,2),(2,3),(3,4),(4,5),(5,6),(6,7)\}. &
\end{array}$$

comes from the sixth Latin square. □

Every affine plane that we know of, has as its order some prime power. We have previously seen (through the connection to MOLS) that there are affine planes of every prime order. Many design theorists have tried to answer the question of whether or not the order of an affine plane must always be a prime power, but the answer is not yet known. In fact, it is not currently known whether or not there is an affine plane of order 12.

EXERCISES 18.28.

1) Prove that if L, M, and N are lines of an affine plane, and L is parallel to both M and N, then M is parallel to N.
2) Draw a finite affine plane of order 5. How many lines does it have?
3) How many points, and how many lines are in a finite affine plane of order 19?
4) Prove the omitted details from the proof of Theorem 18.26: that is, that the given construction yields a structure that satisfies the axioms of an affine plane.

5) Draw an affine plane of order 5. Use the construction given in the proof of Theorem 18.26 to produce 4 mutually orthogonal Latin squares of order 5 from your plane.

18D. Projective planes

A projective plane is another geometric structure (closely related to affine planes). In a finite projective plane, the set of points (and therefore the set of lines) must be finite. Like finite affine planes, finite projective planes can be thought of as a special kind of design.

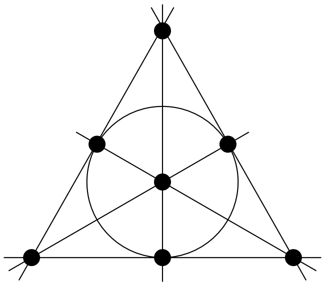
DEFINITION 18.29. A **projective plane** consists of a set of points, a set of lines, and an incidence relation between the points and the lines. The incidence relation must satisfy the following conditions:

- for any two points, there is a unique line that is incident with both of them;
- for any two lines, there is a unique point that is incident with both of them;
- there exist four points such that no three are incident with a single line.

As in the case of affine planes, the final axiom has been developed to avoid some trivial situations.

Think of the points of a finite projective plane as points of a design, and the lines as blocks, with a point being in a block if it is incident with the corresponding line. Then the first condition on the incidence relation for a projective plane guarantees that every pair of points appear together in exactly one block.

EXAMPLE 18.30. The Fano plane is the most well-known finite projective plane (and also the smallest). Here is a drawing of it. It has 7 points and 7 lines, one of which is the circle around the middle.



You have seen this structure already in this course; it is the same as the BIBD$(7, 3, 1)$ that appeared in Example 17.4.

The following is a very interesting connection. We will not try to present the proof here, but it is a natural extension of the similar result that we proved for affine planes.

THEOREM 18.31. *There is a finite projective plane with $n + 1$ points on each line, if and only if there is a complete set of $n - 1$ MOLS of order n.*

EXERCISES 18.32.

1) Is every design with $\lambda = 1$ a projective plane? If not, what condition could fail?
2) Which (if any) of the designs we have seen in this course, are projective planes?
3) From our results on MOLS, for what values can you be sure that a projective plane exists?
4) From our results on MOLS, for what values can you be sure that a projective plane does not exist?

5) What can you determine about the parameters of a design that corresponds to a projective plane?

SUMMARY:

- construction of Steiner triple systems
- structure of affine planes
- connection between affine planes and MOLS
- Important definitions:
  - ○ triple system, Steiner triple system
  - ○ resolvable design, Kirkman triple system
  - ○ t-design
  - ○ affine plane
  - ○ projective plane
- Notation:
  - ○ STS(v)

Chapter 19

Designs and Codes

19A. Introduction

When information is transmitted, it may get garbled along the way. Error-correcting codes can make it possible for the recipient of a garbled message to figure out what the sender intended to say.

ASSUMPTION 19.1. For definiteness, we assume the message to be sent is a string (or "word") of **bits** (0s and 1s). (Information stored in a computer is always converted to such a string, so this is not a serious limitation.)

EXAMPLE 19.2. Perhaps the word 0110 tells an automated factory to close the 2nd and 3rd valves. If we send that message over a wireless network, interference (or some other issue) might change one of the bits, so the factory receives the message 0010. As a result, the factory closes only the 3rd valve, and leaves the 2nd valve open. This could have disastrous consequences, so we would like to do something to avoid such problems.

EXAMPLE 19.3. One simple solution is to append a *check-bit* to the end of the message. To do this, we set three rules:

1) We require all messages to have a certain length. (For example, let's say that all messages must have exactly 5 bits.)
2) We require all messages to have an even number of 1s.
3) We agree that the final bit of the message (called a "parity check-bit") will not convey any information, but will be used only to guarantee that Rule 2 is obeyed. (Thus, each message we send will have 4 bits of information, plus the check bit.)

In particular, if we wish to send the message 0110 (which already has an even number of 1s), then we append 0 to the end, and send the message 01100. If, say, the 2nd bit gets changed in transmission, so the factory receives the message 00100, then the factory's computer control can see that this cannot possibly be the intended message, because it has an odd number of 1s. So the factory can return an error message, asking us to send our instructions again.

Remark 19.4. As a real-life example, bar-code scanners used by cashiers employ the above principle: if the check-bit is not correct, then the scanner does not beep, so the cashier knows that the item needs to be rescanned.

EXERCISE 19.5. Under the rules of Example 19.3, which of the following strings are allowed to be sent as a message?

00110, 10101, 00000, 11011.

It is sometimes not feasible to have a message re-sent (for example, if it spends a long time in transit), so it would be much better to have a system that enables the recipient to *correct* transmission errors, not just *detect* them.

EXAMPLE 19.6 (Triple-repetition code). We could agree to send each bit of our message 3 times. For example, if we want to send the message 0110, then we would transform (or "encode") it as 000111111000. If, say, the 2nd bit gets garbled, so the factory receives 010111111000, then it knows there was a problem in the transmission of the first 3 bits, because they are not all the same. Furthermore, since most of these bits are 0, the factory can figure out that we probably meant to say 000, and correctly decode the entire message as 0110.

The triple-repetition code works, but it is very inefficient, because only one-third of the bits we send are conveying information — most of the bits are check-bits that were added to correct the possible errors. After developing some theory, we will see some codes that are able to correct every single-bit error, but use far fewer check bits.

EXERCISE 19.7. Let $\mathbb{T}^n$ be the set of all ternary sequences of length n (so every entry is 0, 1, or 2). Write a recurrence relation for c_n, the number of code words from $\mathbb{T}^n$ that have no 2 consecutive zeros. Use generating functions to solve your recurrence relation, deriving an explicit formula for c_n.

19B. Error-correcting codes

In order to be able to correct errors in transmission, we agree to send only strings that are in a certain set $\mathcal{C}$ of **codewords**. (So the information we wish to send will need to be "encoded" as one of the codewords.) In our above examples, $\mathcal{C}$ was

- the set of all words of length 5 that have an even number of 1s, or
- the set of words of length 12 that consist of four strings of three equal bits.

The set $\mathcal{C}$ is called a **code**. Choosing the code cleverly will enable us to successfully correct transmission errors.

When a transmission is received, the recipient will assume that the sender transmitted the codeword that is "closest" to the string that was received. For example, if $\mathcal{C}$ were the set of 5-letter words in the English language, and the string "fruiz" were received, then the recipient would assume (presumably correctly), that the sender transmitted the word "fruit," because that is only off by one letter. (This is how we ordinarily deal with the typographical errors that we encounter.)

By the "closest" codeword, we mean the codeword at the smallest distance, in the following sense:

DEFINITION 19.8. Suppose x and y are two bit strings of the same length. The **Hamming distance** from x to y (denoted $d(x, y)$) is the number of bits in which they differ.

EXAMPLE 19.9. For clarity, we underline the bits in the second string that differ from the corresponding bit in the first string:

- $d(11111, 111\underline{0}1) = 1$
- $d(11100, \underline{0}1\underline{0}0\underline{1}) = 3$
- $d(10101, \underline{01010}) = 5$
- $d(10101, 10101) = 0$

Remark 19.10. When two bits are "transposed" (or "switched"), meaning that a string 01 gets changed to 10 (or vice-versa), this counts as two bits being different, because a 0 is changed to a 1 and a 1 is changed to a 0, even though you might think of the switch as being only a single operation.

EXERCISE 19.11. Compute the Hamming distance between the following pairs of words: $\{110, 011\}$, $\{000, 010\}$, $\{\mathrm{brats}, \mathrm{grass}\}$, $\{11101, 00111\}$.

EXERCISE 19.12. Find each of the following:

1) an English word whose Hamming distance from "math" is 0;
2) an English word whose Hamming distance from "math" is 1;
3) an English word whose Hamming distance from "math" is 2;
4) an English word whose Hamming distance from "math" is 3.
5) Can you find more than one of each?

The Hamming distance satisfies the axioms of a "metric" or "distance function:"

EXERCISE 19.13. Prove that the Hamming function satisfies each of the following properties, which define a metric.

Let x, y, and z be words of the same length. Then:

1) $d(x,y) \geq 0$.
2) $d(x,y) = 0 \iff x = y$.
3) $d(x,y) = d(y,x)$.
4) $d(x,z) \leq d(x,y) + d(y,z)$.

Remark 19.14. Part (4) of the Exercise is called the **triangle inequality**, because it says that the length of one side of a triangle is always less than (or equal to) the sum of the lengths of the other two sides.

DEFINITION 19.15. The **minimum distance** of a code $\mathcal{C}$ (denoted $d(\mathcal{C})$) is the smallest Hamming distance between two distinct elements of $\mathcal{C}$.

EXAMPLE 19.16.

1) $d\big(\{10, 010, 011\}\big) = 1$ (because $d(010, 01\underline{1}) = 1$).
2) $d\big(\{000, 011, 101, 110\}\big) = 2$.
3) $d\big(\{10001, 11111\}\big) = 3$.

EXERCISE 19.17. What is the minimum distance of each of the following codes?

1) $\{\mathrm{tell}, \mathrm{tale}, \mathrm{sale}, \mathrm{date}\}$
2) $\{\mathrm{mon}, \mathrm{tue}, \mathrm{wed}, \mathrm{thu}, \mathrm{fri}, \mathrm{sat}, \mathrm{sun}\}$
3) $\{00000, 01011, 10101, 10110, 10011\}$

Making the minimum distance of a code $\mathcal{C}$ large is the key to ensuring that it can detect (or correct) large errors. We will make this idea very explicit in our next two results:

THEOREM 19.18. *A code $\mathcal{C}$ can* ***detect*** *all possible errors affecting at most k bits if and only $d(\mathcal{C}) > k$.*

PROOF. We will prove the contrapositive:

$d(\mathcal{C}) \leq k \iff$ there exists an error that cannot be detected, and affects only k (or fewer) bits.

($\Leftarrow$) Suppose there is a situation in which:

- a codeword x is sent,
- a message y is received,
- with only k incorrect bits, and
- the receiver does not realize that there were any errors.

Since the receiver did not realize there were any errors, the message that was received must be a codeword. In other words, $y \in \mathcal{C}$. Since there are k errors in the received message, we also know that $d(x, y) = k$. Since $x, y \in \mathcal{C}$, this implies $d(\mathcal{C}) \leq k$.

($\Rightarrow$) By assumption, there exist $x, y \in \mathcal{C}$ with $x \neq y$, but $d(x, y) \leq k$. Now, suppose codeword x is sent. Since $d(x, y) \leq k$, changing k (or fewer) bits can change x to y, so y can be the message that is received, even if errors in transmission affect only k bits. Since $y \in \mathcal{C}$, the recipient does not realize an error was made, and assumes that y was the intended message. So the k (or fewer) errors were not detected. □

Although a minimum distance of k allows us to detect errors that affect at most k bits, it isn't sufficient to allow us to correct all such errors. For the purposes of correcting errors, we require the minimum distance to be twice this large.

THEOREM 19.19. *A code $\mathcal{C}$ can* ***correct*** *all possible errors affecting at most k bits if and only $d(\mathcal{C}) > 2k$.*

PROOF. We will prove the contrapositive:

$$d(\mathcal{C}) \leq 2k \iff \begin{array}{c}\text{there exists an error that is not properly corrected,}\\ \text{and affects only } 2k \text{ (or fewer) bits.}\end{array}$$

($\Leftarrow$) Suppose there is a situation in which:

- a codeword x is sent,
- a message y is received,
- with only $2k$ incorrect bits, and
- the receiver decodes the message incorrectly, as some codeword $z \neq x$.

It must be the case that z is the closest codeword to y (or, at least, it ties for being the closest), so $d(z, y) \leq d(x, y) = k$. Then, using Exercise 19.13, we have

$$d(x, z) \leq d(x, y) + d(y, z) = d(x, y) + d(z, y) \leq k + k = 2k.$$

So $d(\mathcal{C}) \leq 2k$ (because $x, z \in \mathcal{C}$).

($\Rightarrow$) By assumption, there exist $x, y \in \mathcal{C}$ with $x \neq y$, but $d(x, y) \leq 2k$. Let $r = \lceil d(x, y)/2 \rceil \leq \lceil 2k/2 \rceil = k$. (In other words, r is obtained by rounding $d(x, y)/2$ *up* to the nearest integer.)

Now suppose codeword x is sent. Since $d(x, y) \leq 2k$, the message y could be received, with no more than $2k$ incorrect bits. Construct z from x by changing only r of the $d(x, y)$ bits that are incorrect in y, so

$$d(x, z) = r \text{ and } d(z, y) = d(x, y) - r.$$

By the definition of r, we have $r \leq d(x, y) \leq 2r$, so

$$d(z, y) = d(x, y) - r \leq 2r - r = r \leq d(x, y).$$

Therefore z is at least as close to y as x is, so the recipient has no way of knowing that x is the message that was sent. So it was not possible to correct the $2k$ (or fewer) errors. □

EXERCISES 19.20.

1) Suppose that a code C has a minimum distance of 7.
   (a) How many errors can it detect?
   (b) How many errors can it correct?
2) Suppose that a code C has a minimum distance of 6.
   (a) How many errors can it detect?
   (b) How many errors can it correct?

EXERCISE 19.21. Let $\mathbb{B}^n$ represent the set of binary strings of length n. Prove that a code from $\mathbb{B}^{10}$ that has more than 2 words, cannot correct 3 errors. Hypothesize a generalisation of this result to codes on $\mathbb{B}^n$ with more than 2 words.

19C. Using the generator matrix for encoding

NOTATION 19.22. It is convenient to represent the binary string $x_1x_2\ldots x_n$ as a *column vector*:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

This allows us to use matrix multiplication to append check bits to a string:

EXAMPLE 19.23. Appending a parity check-bit to the string 010 yields 0101. The same result can be obtained by multiplying the column vector corresponding to 010 by the following **generator matrix**:

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \left[\frac{I_3}{A}\right] \quad \text{where } I_k \text{ is the } k \times k \text{ identity matrix, and } A = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

Namely (calculating all arithmetic modulo 2), we have

$$G \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

In fact, multiplying any 3-bit string by G yields the same string with its parity check-bit appended.

PROOF. $G \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_1 + x_2 + x_3 \end{bmatrix}$, and $x_1 + x_2 + x_3 \pmod 2 = \begin{cases} 0 & \text{if even \# of 1s} \\ 1 & \text{if odd \# of 1s.} \end{cases}$ □

General Method. For some $k, r \in \mathbb{N}^+$,

- choose an $r \times k$ matrix A of 0s and 1s, and
- let $G = \left[\frac{I_k}{A}\right]$.

Multiplying a k-bit string by G yields the same string, with r check bits appended at the end. We let $\mathcal{C}$ be the set of all possible strings Gx, and we call G the **generator matrix** of this code.

Remark 19.24. In the next section, we will see how to choose G so that the resulting code $\mathcal{C}$ can correct errors.

Although many important error-correcting codes are constructed by other methods, we will only discuss the ones that come from generator matrices (except in Section 19E).

DEFINITION 19.25. Any code that comes from a generator matrix G (by the General Method described above) is said to be a **binary linear code**.

EXAMPLE 19.26. Find all the codewords of the binary linear code $\mathcal{C}$ corresponding to the generator matrix

$$G = \left[\frac{I_3}{A}\right], \text{ with } A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

SOLUTION. We have

$$G = \left[\frac{I_3}{A}\right] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

We use this matrix to encode each of the $2^3 = 8$ binary strings of length 3:

$$G\begin{bmatrix}0\\0\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\0\end{bmatrix}, \quad G\begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\1\\1\\1\end{bmatrix}, \quad G\begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\\1\end{bmatrix}, \quad G\begin{bmatrix}0\\1\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\\0\end{bmatrix},$$

$$G\begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\\0\end{bmatrix}, \quad G\begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix}, \quad G\begin{bmatrix}1\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\0\\1\\1\end{bmatrix}, \quad G\begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix}.$$

So $\mathcal{C} = \{00000, 00111, 01001, 01110, 10010, 10101, 11011, 11100\}$. □

EXERCISE 19.27. Encode each of the given words by using the generating matrix $G = \begin{bmatrix} I_k \\ A \end{bmatrix}$ associated to the given matrix A.

1) $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$. Words to encode: 0101, 0010, 1110.

2) $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. Words to encode: 110, 011, 111, 000.

The generator matrix provides an easy way to *encode* messages for sending, but it is hard to use it to *decode* a message that has been received. For that, the next section will introduce a slightly different matrix. From this new matrix, it will be easy to determine whether the corresponding code can correct every single-bit error.

19D. Using the parity-check matrix for decoding

NOTATION 19.28. A binary linear code is of **type (n,k)** (or we say $\mathcal{C}$ is an **(n,k) code**) if its generator matrix $G = \begin{bmatrix} I_k \\ A \end{bmatrix}$ is an $n \times k$ matrix. In other words, G encodes messages of length k as codewords of length n, which means that the number of check bits is $n-k$. We usually use r to denote the number of check bits, so $r = n-k$. Then A is an $r \times k$ matrix.

EXERCISE 19.29. How many codewords are there in a binary linear code of type (n,k)?

DEFINITION 19.30. If $G = \begin{bmatrix} I_k \\ A \end{bmatrix}$ is the generator matrix of a binary linear code $\mathcal{C}$, and A is an $r \times k$ matrix (so $\mathcal{C}$ is of type $(k+r,k)$), then the **parity-check matrix** of $\mathcal{C}$ is

$$P = [A \; I_r].$$

EXAMPLE 19.31.

1) For the code $\mathcal{C}$ of Example 19.26, the matrix A is 2×3, so $r = 2$. Therefore, the parity-check matrix of $\mathcal{C}$ is

$$P = [A \; I_r] = [A \; I_2] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

2) For a single parity check-bit, as in Example 19.23, we have $A = [1\;1\;1]$. This is a 1×3 matrix, so $r = 1$. Therefore, the parity-check matrix of the code is

$$P = [A \; I_r] = [A \; I_1] = [1\;1\;1\;1]$$

(since $I_1 = [1]$).

EXERCISE 19.32. Suppose the generator matrix of the binary linear code $\mathcal{C}$ is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

What is the parity-check matrix of this code?

The parity-check matrix can be used to check whether a message we received is a valid codeword:

PROPOSITION 19.33. *A column vector x is a codeword if and only if $Px = 0$.*

PROOF. ($\Rightarrow$) Since x is a codeword, we have $x = Gm$ for some (k-bit) message m. This means that

$$x = Gm = \begin{bmatrix} I_k \\ A \end{bmatrix} m = \begin{bmatrix} m \\ Am \end{bmatrix}.$$

Then

$$Px = [A \ I_r] \begin{bmatrix} m \\ Am \end{bmatrix} = \begin{bmatrix} Am + Am \end{bmatrix} = \begin{bmatrix} 2Am \end{bmatrix} \equiv 0 \pmod 2.$$

($\Leftarrow$) Suppose $Px = 0$. Write $x = \begin{bmatrix} m \\ y \end{bmatrix}$, where

- m is the first k rows of x, and
- y is the remaining $r = n - k$ rows of x.

Then

$$0 = Px = [A \ I_r] \begin{bmatrix} m \\ y \end{bmatrix} = \begin{bmatrix} Am + y \end{bmatrix}.$$

This means $y = -Am = Am \pmod 2$, so

$$x = \begin{bmatrix} m \\ y \end{bmatrix} = \begin{bmatrix} m \\ Am \end{bmatrix} = \begin{bmatrix} I_k \\ A \end{bmatrix} m = Gm,$$

so $x \in \mathcal{C}$. □

EXAMPLE 19.34. Here is a simple illustration of Proposition 19.33. For the code in which every codeword is required to have an even number of 1s, Example 19.31(2) tells us that the parity-check matrix is $P = [1\ 1\ 1\ 1]$. Hence, for any 4-bit string $x_1x_2x_3x_4$, we have

$$Px = [1\ 1\ 1\ 1] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = [x_1 + x_2 + x_3 + x_4].$$

This is 0 (mod 2) if and only if there are an even number of 1s in x, which is what it means to say that x is a codeword.

EXAMPLE 19.35. Use the parity-check matrix to determine whether each of these words is in the code $\mathcal{C}$ of Example 19.26:

11111, 10101, 00000, 11010.

SOLUTION. From Example 19.31(1), we know that the parity-check matrix of this code is

$$P = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

We have:

- $P \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, so 11111 is not a codeword.
- $P \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, so 10101 is a codeword.

- $P \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 \\ 0 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, so 00000 is a codeword.
- $P \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 \\ 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, so 11010 is not a codeword.

(These answers can be verified by looking at the list the elements of $\mathcal{C}$ in the solution of Example 19.26.) □

It is evident from the parity-check matrix whether a code corrects every single-bit error:

THEOREM 19.36. *A binary linear code $\mathcal{C}$ can correct every single-bit error if and only if the columns of its parity-check matrix are all distinct and nonzero.*

PROOF. Suppose a codeword x is transmitted, but the ith bit gets changed, so a different string y is received. Let e_i be the string that is all 0s, except that the ith bit is 1, so $y = x + e_i$. Then

$$Py = P(x + e_i) = Px + Pe_i = 0 + Pe_i = Pe_i$$

is the ith column of P.

Therefore, if all the columns of P are nonzero, then Py is nonzero, so the receiver can detect that there was an error. If, in addition, all of the columns of P are distinct, then Py is equal to the ith column of P, and not equal to any other column, so the receiver can conclude that the error is in the ith bit. Changing this bit corrects the error.

Conversely, if either the ith column of P is zero, or the ith column is equal to the jth column, then either $Pe_i = 0$ or $Pe_i = Pe_j$. Therefore, when the codeword $00\ldots0$ is sent, and an error changes the ith bit, resulting in the message e_i being received, either $Pe_i = 0$, so the receiver does not detect the error (and erroneously concludes that the message e_i is what was sent), or cannot tell whether the error is in the ith bit (and message 0 was sent) or the error is in the j th bit (and message $e_i + e_j$ was sent). In either case, this is a single-bit error that cannot be corrected. □

EXERCISE 19.37. The parity-check matrix of the binary linear code $\mathcal{C}$ is

$$P = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Can $\mathcal{C}$ correct all single-bit errors?

The proof of Theorem 19.36 shows how to correct any single-bit error (when it is possible):

General Method. Assume the word y has been received. Calculate Py.

- If $Py = 0$, then y is a codeword. Assume there were no errors, so y is the codeword that was sent.
- Now suppose $Py \neq 0$.
  - ○ If Py is equal to the ith column of P, then let $x = y + e_i$. (In other words, create x by changing the ith bit of y from 0 to 1 or vice-versa.) Then x is a codeword. Assume it is the codeword that was sent.

- ○ If Py is not equal to any of the columns of P, then at least two of the bits of y are wrong. Do not try to correct the error.

EXAMPLE 19.38. Suppose the parity-check matrix of a binary linear code is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Decode each of the following received words:

$$111000,\ 101001,\ 001101.$$

SOLUTION. Let P be the given parity-check matrix. Then:

- $P \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$ This is the 4th column of P, so changing the 4th bit corrects the error. This means that the received word 111000 decodes as $111\underline{1}00$.
- $P \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$ This is 0, so there is no error. This means that the received word 101001 decodes as 101001.
- $P \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$ This is not any of the columns of P, so there are at least two errors. Therefore, we cannot decode the received word 001101.

EXERCISES 19.39.

1) The parity-check matrix of a certain binary linear code is

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(a) Decode each of the following received words: 10001111, 11110000, 01111101.

(b) Find the generator matrix of the code.

2) The parity check matrix of a certain binary linear code is

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

(a) Can the code correct all single-bit errors?

(b) Decode each of the following received words: 001001, 110011, 000110.

EXAMPLE 19.40. Let

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

This is a 4×11 matrix whose columns list all of the binary vectors of length 4 that have at least two 1s. The corresponding 4×15 parity-check matrix $P = [A\ I_4]$ lists all $2^4 - 1 = 15$ nonzero binary vectors of length 4 (without repetition), so the resulting binary linear code can correct all single-bit errors.

The corresponding generator matrix $G = \begin{bmatrix} I_{11} \\ A \end{bmatrix}$ is a 15×11 matrix, so it takes an 11-bit message, and adds only $15 - 11 = 4$ check bits. This is much more efficient than the triple-repetition code of Example 19.6, which would have to add 22 check bits to detect every single-bit error in an 11-bit message.

Remark 19.41. Generalizing Example 19.40, a binary linear code is called a **Hamming code** if the columns of its parity-check matrix $P = [A\ I_r]$ are a list of all the $2^r - 1$ nonzero binary vectors of length r (in some order, and without repetition). Every Hamming code can correct all single-bit errors. Because of their high efficiency, Hamming codes are often used in real-world applications. But they only correct single-bit errors, so other binary linear codes (which we will not discuss) need to be used in situations where it is likely that more than one bit is wrong.

EXERCISES 19.42.

1) Explain how to make a binary linear code of type $(29, 24)$ that corrects all single-bit errors.
2) Explain why it is impossible to find a binary linear code of type $(29, 25)$ that corrects all single-bit errors.
3) For each $k \leq 20$, find the smallest possible number r of check bits in a binary linear code that will let you send k-bit messages and correct all single-bit errors. (That is, for each k, we want a code of type (n, k) that corrects all single-bit errors, and we want $r = n - k$ to be as small as possible.)
4) What is the smallest possible number r of check bits in a binary linear code that will let you send 100-bit messages and correct all single-bit errors?

19E. Codes from designs

An error-correcting code can be constructed from any design BIBD(v, k, λ) for which $\lambda = 1$. Namely, from each block of the design, create a binary string of length v, by placing a 1 in each of the positions that correspond to points in the design, and 0s everywhere else. (However, this will not usually have a generator matrix, so it is not a binary linear code.)

EXAMPLE 19.43. For the BIBD$(7, 3, 1)$ that has arisen in previous examples, with blocks

$$\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\},$$

the corresponding code is

$$\mathcal{C} = \{1110000, 1001100, 1000011, 0101010, 0100101, 0011001, 0010110\}.$$

PROPOSITION 19.44. *A BIBD$(v, k, 1)$ can be used to produce a code that can correct up to $k - 2$ errors.*

PROOF. Let B and B' be blocks of the design, and let b, b' be the corresponding binary strings of length k as described at the start of this section. If the blocks have no points in common, then $d(b, b') = 2k$. If the blocks have 1 entry in common, then

$$d(b, b') = 2(k-1)$$

(the strings differ in the $k-1$ positions corresponding to points that are in B but not in B', and in the $k-1$ positions corresponding to points that are in B' but not in B). Since $\lambda = 1$, the blocks cannot have more than one point in common. So in any case,

$$d(b, b') \geq 2(k-1).$$

Since b and b' were arbitrary output words of the code (because B and B' were arbitrary blocks), this means that $d(\mathcal{C}) \geq 2(k-1)$. This is greater than $2(k-2)$, so Theorem 19.19 tells us that the code can correct any $k-2$ errors. □

EXERCISES 19.45.

1) If you use a BIBD to create a code whose words have length 10, that is 4-error-correcting. How many words will your code have?

2) How many errors can be corrected by a code that comes from a BIBD$(21, 4, 1)$?

3) Recall the 2-$(8, 4, 3)$ design given in Exercise 17.20(2). It is possible to show that this is also a 3-$(8, 4, 1)$ design; for the purposes of this problem, you may assume that this is true. If we convert these blocks to binary strings to form code words for a code, how many errors can this code correct?

SUMMARY:

- Important definitions:
  - ○ binary string
  - ○ code, codeword
  - ○ Hamming distance
  - ○ minimum distance of a code
  - ○ detect errors, correct errors
  - ○ encode, decode
  - ○ generator matrix
  - ○ parity-check matrix
  - ○ binary linear code of type (n, k)
  - ○ Hamming code
- Notation:
  - ○ $d(x, y)$
  - ○ $d(\mathcal{C})$
  - ○ $G = \begin{bmatrix} I_k \\ A \end{bmatrix}$
  - ○ $P = [A \ I_r]$

Index

List of Notation

$n!$, 19

$\binom{n}{r}$, 22

$\left(\!\binom{n}{r}\!\right)$, 35

$\binom{n}{r_1,\ldots,r_m}$, 37

(IH), 42

V, 87

E, 87

$E(G)$, 87

$V(G)$, 87

$u \sim v$, 88

uv, 88

$\mathrm{val}(v)$, 88

$\deg(v)$, 88

$d(v)$, 88

$d_G(v)$, 88

$G \setminus \{v\}$, 90

$G \setminus S$, 90

$G \setminus \{e\}$, 90

K_n, 90

$\varphi : G_1 \to G_2$, 93

$G_1 \cong G_2$, 93

P_n, 103

C_n, 104

δ, 115

Δ, 115

$\delta(G)$, 115

$\Delta(G)$, 115

$\chi'(G)$, 120

χ', 120

$K_{m,n}$, 121

$c(v)$, 123

$R(n_1, \ldots, n_c)$, 127

$\chi(G)$, 129

χ, 129

$F(G)$, 136

F, 136

G^*, 136

MOLS, 153

$a \equiv b \pmod{n}$, 154

$\mathcal{B}$, 163

v, 163

b, 163

r, 163

k, 163

λ, 163

(b, v, r, k, λ)-design, 163

BIBD, 164

BIBD(v, k, λ), 164

STS(v), 173

Appendix A

Solutions to selected exercises

For the reader's convenience, solutions below are given with full work shown as well as a final numerical solution. Typically the final numerical solution would not be expected, but makes it easier to verify an answer that has been reached using a different method.

Solutions for Chapter 2

Solutions to Exercise 2.7.

1) There are 4 choices for colour; 2 choices for air conditioning; 5 choices for stereo; and 3 choices for floor mats. So in total, there are $4 \cdot 2 \cdot 5 \cdot 3 = 120$ different combinations of options. Of these, 3 combinations are available at the dealership, so the probability that one of these cars has the options he wants is $3/120 = 1/40$.

2) In Candyce's book, the reader will have 3 choices at the first decision point, and 2 choices at each of the following three decision points. Thus, there are a total of $3 \cdot 2 \cdot 2 \cdot 2 = 3 \cdot 2^3 = 24$ possible storylines. Candyce must write 24 endings.

Solutions to Exercise 2.13.

1) Let's call the black markers Black A, Black B, and Black C. The four possible options are: I leave behind the blue marker; I leave behind Black A; I leave behind Black B; I leave behind Black C. In each of the final three cases, I take the blue marker. Therefore, the probability that I take the blue marker is $(1 + 1 + 1)/4 = 3/4$.

2) If Maple is thinking of a letter, there are 26 things she could be thinking of. If she is thinking of a digit, there are 10 things she could be thinking of. In total, there are $10 + 26 = 36$ things she could be thinking of.

Solutions to Exercise 2.17.

1) We divide the possible passwords into three cases, depending on whether the digit is in the first, second, or third position. In each case, we have 10 choices for the digit, 26 choices for the first lowercase letter, and 26 choices for the second lowercase letter. Thus, in each case we have $10 \cdot 26^2$ possible passwords. In total, there are $10 \cdot 26^2 + 10 \cdot 26^2 + 10 \cdot 26^2 = 30 \cdot 26^2 = 20,280$ different passwords with these constraints.

2) We divide the possible passwords into two cases, depending on whether there are 8 or 9 characters. If there are 8 characters, then the product rule tells us that there are 10^8 passwords consisting entirely of digits (10 choices for the digit in each of the 8 positions). Similarly, if there are 9 characters, then there are 10^9 passwords consisting entirely of digits. In total, there are $10^8 + 10^9 = 1,100,000,000$ passwords with these constraints.

Solutions to Exercise 2.19. It is sometimes possible to turn a use of the sum rule into a use of the product rule, or vice versa, so you might get different answers that could be correct. The answers below represent one natural way of solving each problem.

1) Use both rules. There are two cases that should be added together: the number of numbers that have two digits, and the number of numbers that have four digits. For each of these cases, use the product rule to determine how many numbers have this property. (The answer is $9 \cdot 10 + 9 \cdot 10^3 = 9,090$. Note that in order for a number to have exactly k digits, the leading digit cannot be zero.)

2) Use only the product rule. There are 6 outcomes from the red die, and for each of these, there are 6 outcomes from the yellow die, for a total of $6 \cdot 6 = 36$ outcomes.

Solutions for Chapter 3

Solutions to Exercise 3.8.

1) The band may choose any one of the 6 people to play lead guitar. They may then choose any one of the remaining 5 people to play bass. Therefore, the band can be completed in $6 \cdot 5 = 30$ ways. You might also observe that the number of ways to complete the band is the number of 2-permutations (for the two open spots) of 6 people, which is $6 \cdot \ldots \cdot (6-2+1) = 6 \cdot 5 = 30$.

2) Divide this into two cases, depending on which of the two parts Garth got. If he got the first part, then there were 8 other people competing for 4 other roles, so the number of ways of completing the cast in this case is the number of 4-permutations of the 8 people. Repeating this argument for the second case (if Garth got the other part) and adding the two numbers, we see that in total there are $2 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ (since $8-4+1=5$) ways of completing the cast. This works out to $3,360$.

Solutions to Exercise 3.15.

2) At the end of this trick, the only sets of cards that she could not possibly end up with are sets that contain nothing but spades. There are $\binom{13}{3}$ sets that include only spades (choose any 3 of the 13 spades), and $\binom{52}{3}$ possible sets of 3 cards from the deck as a whole, so the number of sets of three cards that are not all spades is $\binom{52}{3} - \binom{13}{3} = 22,100 - 286 = 21,814$.

3) The leading digit cannot be a zero, so if there are to be exactly two zeroes, we have 4 possible positions in which they can be placed. Thus, there are $\binom{4}{2}$ ways of choosing where to place the two zeroes. In each of the remaining three positions, we can place any of the digits 1 through 9, so there are 9^3 choices for the remaining digits. Thus, there are $\binom{4}{2}9^3 = 4,374$ 5-digit numbers that contain exactly two zeroes.

Solutions to Exercise 3.21.

2) Using the Binomial Theorem, we see that

$$(a+b)^5(c+d)^6 = \left(\sum_{r=0}^{5} \binom{5}{r} a^r b^{5-r}\right)\left(\sum_{s=0}^{6} \binom{6}{s} c^s d^{6-s}\right).$$

To find the coefficient of $a^2b^3c^2d^4$, we must take $r = 2$ and $s = 2$. This gives us the term $\binom{5}{2}a^2b^3\binom{6}{2}c^2d^4 = \binom{5}{2}\binom{6}{2}a^2b^3c^2d^4$. Thus, the coefficient of $a^2b^3c^2d^4$ is $\binom{5}{2}\binom{6}{2} = 10 \cdot 15 = 150$.

4) Using the Binomial Theorem, we see that

$$(a+b)^5 + (a+b^2)^4 = \sum_{r=0}^{5}\binom{5}{r}a^r b^{5-r} + \sum_{s=0}^{4}\binom{4}{s}a^s(b^2)^{4-s}.$$

The coefficient of a^3b^2 in the first summand arises when $r = 3$; in the second summand, it arises when $s = 3$. This gives us the term $\binom{5}{3}a^3b^2 + \binom{4}{3}a^3(b^2)^1$. Thus, the coefficient of a^3b^2 is $\binom{5}{3} + \binom{4}{3} = 10 + 4 = 14$.

Solutions for Chapter 4

Solutions to Exercise 4.3.

1) When counting the number of subsets of an n-set, we saw that there is a bijection between that number and the number of binary strings of length n: identify each element of the set with a position in the string, and put a 0 in that position if the element is not in the subset, and a 1 if it is.

   Analogously, we can find a bijection between the number of these structures and the number of ternary strings of length n (strings containing 0, 1, or 2 in each position). Identify each element of the set with a position in the string, put a 0 in that position if the element is not in the structure, a 1 if it occurs once, and a 2 if it occurs twice. Thus, we can form 3^n structures from the set $\{1, \ldots, n\}$: there are 3 choices for each of the n entries in the ternary string.

3) We identify each of the ten Olympic contenders with a crib, and each of the three dolls with one of the three medals. If the doll corresponding to the gold medal goes into crib i, this corresponds to the competitor corresponding to crib i winning the gold medal. Similarly, if the doll corresponding to the silver medal goes into crib j, this is equivalent to the contender corresponding to crib j winning the silver medal; and the doll corresponding to bronze going into crib k is equivalent to the contender corresponding to crib k winning the bronze medal.

Solutions to Exercise 4.11.

2) **COMBINATORIAL PROOF.** We use the problem given to us in the hint, so will be counting the number of ways to start with n dogs, determine r who will enter a competition and k of those who will be finalists.

   Counting method 1: From the n dogs, we first choose the r who will enter the competition. This can be done in $\binom{n}{r}$ ways. For each of these ways, we can choose k of the r competitors to become finalists in $\binom{r}{k}$ ways. Thus, there are a total of $\binom{n}{r}\binom{r}{k}$ ways to choose the dogs.

Counting method 2: From the n dogs, choose k who will be the finalists. This can be done in $\binom{n}{k}$ ways. For each of these ways, we can look at the remaining $n-k$ dogs and choose $r-k$ to be the competitors who will not be finalists, in $\binom{n-k}{r-k}$ ways. Thus, there are a total of $\binom{n}{k}\binom{n-k}{r-k}$ ways to choose the dogs.

Since both of these solutions count the answer to the same problem, the answers must be equal, so we have $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$. □

3) **COMBINATORIAL PROOF.** We will count the number of ways to choose a random sample of n people from a class of n men and n women.

Counting method 1: From the $2n$ total people, choose n of them for the random sample. This can be done in $\binom{2n}{n}$ ways.

Counting method 2: Let r represent the number of men who will be in the sample. Notice that r may have any value from 0 up to n. We divide the problem into these $n+1$ cases, and take the sum of all of the answers. In each case, we can choose the r men for the sample from the n men, in $\binom{n}{r}$ ways. For each of these ways, from the n women, we choose r who will not be part of the sample (so the remaining $n-r$ will be in the sample, for a total of $r+n-r=n$ people in the sample). There are $\binom{n}{r}$ ways to do this. Thus the total number of ways of choosing r men and $n-r$ women for the sample is $\binom{n}{r}^2$. Adding up the solutions for all of the cases, we obtain a final answer of $\sum_{r=0}^{n}\binom{n}{r}^2$.

Since both of these solutions count the answer to the same problem, the answers must be equal, so we have $\sum_{r=0}^{n}\binom{n}{r}^2 = \binom{2n}{n}$. □

Solutions to Exercise 4.12.

1) We could use this expression to count the number of ways of choosing one leader and some number (which could be zero) of other team members for a project, from a group of n people. There are n ways to choose the leader, and for each of these, there are 2^{n-1} ways of choosing a subset of the other $n-1$ people to be team members.

3) We could use this expression to count the number of ways of starting with a collection of n books, choosing r books to put out on bookshelves and some other number (which could be zero) of other books to keep but not display. We break this down into cases depending on the total number k of books that are kept (including the displayed books), which could be anywhere from r up to n. We will take the sum of all of the answers. In each case, there are $\binom{n}{k}$ ways of choosing the k books to keep, and for each such

choice, there are $\binom{k}{r}$ ways of choosing the r books to display from the books that are kept. Thus, there are a total of $\sum_{k=r}^{n}\binom{n}{k}\binom{k}{r}$ solutions to this problem.

Solutions for Chapter 5

Solutions to Exercise 5.5.

2) There are 6^3 ways for the teacher gifts to be chosen (each child can choose any one of the six types of prizes to give to his teacher). There are $\left(\!\binom{6}{3}\!\right)$ ways for Kim to choose his other three prizes; $\left(\!\binom{6}{2}\!\right)$ ways for Jordan to choose his other two prizes, and $\left(\!\binom{6}{5}\!\right)$ ways for Finn to choose his other five prizes. Thus, the total number of ways for the prizes (including teacher gifts) to be chosen is

$$\begin{aligned} 6^3\left(\!\binom{6}{3}\!\right)\left(\!\binom{6}{2}\!\right)\left(\!\binom{6}{5}\!\right) &= 6^3\binom{6+3-1}{3}\binom{6+2-1}{2}\binom{6+5-1}{5} \\ &= 6^3\binom{8}{3}\binom{7}{2}\binom{10}{5} \\ &= 6^3\cdot 56\cdot 21\cdot 252 = 64,012,032. \end{aligned}$$

3) Since the judges must choose at least one project from each age group, this is equivalent to a problem in which they are choosing only six projects to advance, with no restrictions on how they choose them. They can choose six projects from three categories in $\left(\!\binom{3}{6}\!\right) = \binom{3+6-1}{6} = \binom{8}{6} = 28$ ways.

Solutions to Exercise 5.6.

1) **COMBINATORIAL PROOF.** We will count the number of ways of choosing k items from a menu that has n different entries (including mac and cheese), in two ways.

Counting method 1: By definition, the answer to this is $\left(\!\binom{n}{k}\!\right)$.

Counting method 2: We divide our count into two cases, according to whether or not we choose any orders of mac and cheese. If we do not choose any mac and cheese, then we must choose our k items from the other $n-1$ entries on the menu. We can do this in $\left(\!\binom{n-1}{k}\!\right)$ ways. If we do choose at least one order of mac and cheese, then we must choose the other $k-1$ items from amongst the n entries on the menu (with mac and cheese still being an option for additional choices). We can do this in $\left(\!\binom{n}{k-1}\!\right)$ ways. By the sum rule, the total number of ways of making our selection is $\left(\!\binom{n-1}{k}\!\right) + \left(\!\binom{n}{k-1}\!\right)$.

Since both of these methods are counting the same thing, the answers must be equal, so $\left(\!\binom{n}{k}\!\right) = \left(\!\binom{n-1}{k}\!\right) + \left(\!\binom{n}{k-1}\!\right)$. □

Solutions to Exercise 5.12.

1) There are 14 words in the list. The word "the" appears three times; the words "on" and "child" appear twice each; the other seven words each appear once. Thus, the number of "poems" (orderings of the set) is

$$\binom{14}{3,2,2,1,1,1,1,1,1,1} = \frac{14!}{3!2!2!} = 3,632,428,800.$$

Solutions for Chapter 6

Solutions to Exercise 6.6.

1) Various formulas are possible. Most simply, the sequence can be described by the recurrence relation $s_1 = 4$, $s_i = 2s_{i-1} + 1$ for $i \geq 2$. With this description, the next term is $s_5 = 2(39) + 1 = 79$.

3) Adjusting the recurrence relation from Example 6.5, we obtain the new relation

$$r_n = r_{n-1} - 20 + .01(r_{n-1} - 20).$$

This simplifies to $r_n = 1.01(r_{n-1} - 20)$. We still have $r_0 = 2000$. We now have

$$r_1 = 1.01(r_0 - 20) = 1.01(1980) = 1999.80.$$

Stavroula is (marginally) losing money from the beginning. This situation will only get worse as her starting balance each year dwindles.

Solutions to Exercise 6.12.

1) **PROOF.** Base case: $n = 1$. We have $b_1 = 5$ and $5 + 4(1 - 1) = 5$, so $b_n = 5 + 4(n - 1)$ when $n = 1$.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 1$ be arbitrary, and suppose that the equality holds for $n = k$; that is, assume that $b_k = 5 + 4(k - 1)$.

Now we want to deduce that

$$b_{k+1} = 5 + 4(k + 1 - 1) = 5 + 4k.$$

Using the recursive relation, we have $b_{k+1} = b_k + 4$ since $k + 1 \geq 2$. Using the inductive hypothesis, we have $b_k = 5 + 4(k - 1)$. Putting these together gives

$$b_{k+1} = 5 + 4(k - 1) + 4 = 5 + 4k - 4 + 4 = 5 + 4k = 5 + 4(k + 1 - 1),$$

as desired. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $b_n = 5 + 4(n - 1)$ for every $n \geq 1$. □

3) **PROOF.** Base case: $n = 0$. We have $0! = 1$ (by definition) and $n = 0$, so $n! = 1 \geq 0 = n$. Thus, $n! \geq n$ when $n = 0$.

Inductive step: We begin with the inductive hypothesis. Let $k \geq 0$ be arbitrary, and suppose that the inequality holds for $n = k$; that is, assume that $k! \geq k$.

Now we want to deduce that $(k + 1)! \geq k + 1$. Using the definition of factorial, we have $(k + 1)! = (k + 1)k!$ since $k + 1 \geq 0 + 1 = 1$. Using the inductive hypothesis, we have $k! \geq k$. Putting these together gives

$$(k + 1)! = (k + 1)k! \geq (k + 1)k.$$

If $k \geq 1$, then

$$(k + 1)k \geq (k + 1)1 = k + 1$$

and we are done. If $k = 0$, then $(k + 1)! = 1! = 1 = k + 1$ and again the inequality is satisfied. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $n! \geq n$ for every $n \geq 0$. □

Solutions to Exercise 6.17.

2) **PROOF.** Base cases: We will have four base cases: $n = 12$, $n = 13$, $n = 14$, and $n = 15$.

For $n = 12$, I can get \$12 onto my gift card by buying three increments of \$4, since $4 + 4 + 4 = 12$.

For $n = 13$, I can get \$13 onto my gift card by buying two increments of \$4 and one of \$5, since $4 + 4 + 5 = 13$.

For $n = 14$, I can get \$14 onto my gift card by buying two increments of \$5 and one of \$4, since $4 + 5 + 5 = 14$.

For $n = 15$, I can get \$15 onto my gift card by buying three increments of \$5, since $5 + 5 + 5 = 12$.

Inductive step: We begin with the (strong) inductive hypothesis. Let $k \geq 15$ be arbitrary, and assume that for every integer i with $k - 3 \leq i \leq k$, I can put \$$i$ onto my gift card.

Now I want to deduce that I can put \$$(k+1)$ onto my gift card. Using the inductive hypothesis in the case $i = k - 3$, I see that add can put \$$(k - 3)$ onto my gift card by buying increments of \$4 or \$5. Now if I buy one additional increment of \$4, I have put a total of \$$(k - 3 + 4)$ = \$$(k + 1)$ onto my gift card, as desired. This completes the proof of the inductive step.

By the (strong) Principle of Mathematical Induction, I can put any amount of dollars that is at least \$12 onto my gift card. □

Solutions for Chapter 7

Solutions to Exercise 7.3.

2) Since the nth term of the sequence is 2^n, the generating function is $\sum_{n=0}^{\infty} 2^n x^n$.

3) The generating function is $1 + 5x + 10x^2 + 15x^3 + 10x^4 + 5x^5 + x^6$.

Solutions to Exercise 7.10.

1) We have

$$\binom{-5}{7} = (-1)^7 \binom{5 + 7 - 1}{7} = -\binom{11}{7} = -330.$$

2) By the Generalised Binomial Theorem, the coefficient of y^4 in $(1 + y)^{-2}$ is $\binom{-2}{4}$, so (replacing y with $-x$) the coefficient of x^4 in $(1 - x)^{-2}$ is

$$(-1)^4 \cdot \binom{-2}{4} = (1) \cdot \frac{(-2)(-3)(-4)(-5)}{4!} = 5.$$

Solutions to Exercise 7.15.

1) **PROOF.** Base case: $n = 1$. The left-hand side of the equation in this case is $1+x$. The right-hand side is $\frac{1-x^2}{1-x}$. Since $1-x^2 = (1-x)(1+x)$, we can rewrite the right-hand side as $\frac{(1-x)(1+x)}{1-x}$. Cancelling the $1-x$ from the top and bottom gives $1+x$, so the two sides are equal. Since a generating function is a formal object, x is acting as a placeholder, and we do not need to worry about the possibility that $1-x=0$ that would prevent us from cancelling these factors.

Inductive step: Let $k \geq 1$ be arbitrary, and suppose that

$$1+\cdots+x^k = \frac{1-x^{k+1}}{1-x}.$$

Now we must deduce that

$$1+\cdots+x^{k+1} = \frac{1-x^{k+2}}{1-x}.$$

We have

$$1+\cdots+x^{k+1} = (1+\cdots+x^k)+x^{k+1}.$$

Applying our inductive hypothesis, this is $\frac{1-x^{k+1}}{1-x}+x^{k+1}$. Adding this up over a common denominator of $1-x$ gives

$$\frac{1-x^{k+1}+x^{k+1}-x^{k+2}}{1-x} = \frac{1-x^{k+2}}{1-x},$$

as desired.

By the Principle of Mathematical Induction,

$$1+\cdots+x^n = \frac{1-x^{n+1}}{1-x}$$

for every $n \geq 1$. □

4) The generating function for this problem is

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

We can rewrite this as

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

Finding the coefficient of x^{11} in this expression is equivalent to finding the coefficient of x^6 in

$$(1+x+x^2+x^3+x^4+x^5)^5 = \left(\frac{1-x^6}{1-x}\right)^5.$$

Using the Binomial Theorem and substituting $y=-x^6$, we see that

$$\begin{aligned}(1-x^6)^5 &= (-x^6)^0+\binom{5}{1}(-x^6)^1+\binom{5}{2}(-x^6)^2+\binom{5}{3}(-x^6)^3+\binom{5}{4}(-x^6)^4+(-x^6)^5\\ &= 1-5x^6+10x^{12}-10x^{18}+5x^{24}-x^{30}.\end{aligned}$$

The function we're interested in is the product of this with $(1-x)^{-5}$, and we are looking for the coefficient of x^6. The only ways of getting an x^6 term from this product are by taking the x^0 term above and multiplying it by the x^6 term from $(1-x)^{-5}$, or by taking the x^6 term above and multiplying it by the x^0 term from $(1-x)^{-5}$.

Using the Generalised Binomial Theorem (and substituting $y = -x$), the coefficient of x^0 in $(1-x)^{-5}$ is

$$(-1)^0\binom{-5}{0} = (-1)^0(-1)^0\binom{5+0-1}{0} = 1.$$

Similarly, the coefficient of x^6 in $(1-x)^{-5}$ is

$$(-1)^6\binom{-5}{6} = (-1)^6(-1)^6\binom{5+6-1}{6} = \binom{10}{6} = 210.$$

Thus, the number of ways in which Trent can roll a total of 11 on his five dice is the coefficient of x^{11} in our generating function, which is $\binom{10}{6} - 5 = 205$. The probability of this happening is 205 divided by the total number of outcomes of his roll, which is $6^5 = 7776$, so 205/7776, or about 2.5%.

Solutions for Chapter 8

Solutions to Exercise 8.2.

1) First we rewrite the generating function as a sum of two parts:

$$\frac{1}{(1+2x)(2-x)} = \frac{A}{1+2x} + \frac{B}{2-x} = \frac{A(2-x)+B(1+2x)}{(1+2x)(2-x)}.$$

Now the numerator gives $2A + B + (2B - A)x = 1$ as polynomials. Hence we must have $2B - A = 0$ and $2A + B = 1$. Combining these gives $B = 1/5$ and $A = 2/5$. Thus the given generating function is equal to

$$\frac{2}{5}(1+2x)^{-1} + \frac{1}{5}(2-x)^{-1} = \frac{2}{5}(1+2x)^{-1} + \frac{1}{10}(1-\frac{1}{2}x)^{-1}.$$

Using the Generalised Binomial Theorem, the coefficient of x^r in the first of these summands is $\frac{2}{5}(-1)^r2^r$, while the coefficient of x^r in the second summand is $\frac{1}{10}\left(\frac{1}{2}\right)^r$. Thus, the coefficient of x^r is $\frac{2}{5}(-1)^r2^r + \frac{1}{10}\left(\frac{1}{2}\right)^r$.

3) First we rewrite the generating function as a sum of three parts:

$$\begin{aligned}\frac{1+2x}{(1-2x)(2+x)(1+x)} &= \frac{A}{1-2x} + \frac{B}{2+x} + \frac{C}{1+x} \\ &= \frac{A(2+x)(1+x) + B(1-2x)(1+x) + C(1-2x)(2+x)}{(1-2x)(2+x)(1+x)}.\end{aligned}$$

Now the numerator gives

$$\begin{aligned}&A(2+3x+x^2) + B(1-x-2x^2) + C(2-3x-2x^2) \\ = \;& 2A + B + 2C + (3A - B - 3C)x + (A - 2B - 2C)x^2 \quad = 1 + 2x\end{aligned}$$

as polynomials, so we have $2A + B + 2C = 1$, $3A - B - 3C = 2$, and $A - 2B - 2C = 0$. Solving this gives $C = -1/3$, $B = 3/5$, and $A = 8/15$. Thus (taking a factor of 2 out of the denominator of the second piece) the given generating function is equal to

$$\frac{8}{15}(1-2x)^{-1} + \frac{3}{10}(1+\frac{1}{2}x)^{-1} - \frac{1}{3}(1+x)^{-1}.$$

Using the Generalised Binomial Theorem, the coefficient of x^r in the first of these summands is $\dfrac{8}{15}2^r$; the coefficient of x^r in the second summand is $\dfrac{3}{10}(-1)^r\left(\dfrac{1}{2}\right)^r$; and the coefficient of x^r in the third summand is $-\dfrac{1}{3}(-1)^r$. We conclude that the coefficient of x^r in this generating function is

$$\frac{8}{15}2^r + \frac{3}{10}(-1)^r\left(\frac{1}{2}\right)^r - \frac{1}{3}(-1)^r.$$

Solutions to Exercise 8.5.

2) To use the method of partial fractions, we first factor the denominator:

$$2x^2 + x - 1 = (2x-1)(x+1).$$

Now, write

$$\begin{aligned} f(x) &= \frac{2+x}{2x^2+x-1} = \frac{2+x}{(2x-1)(x+1)} = \frac{A}{2x-1} + \frac{B}{x+1} \\ &= \frac{A(x+1)+B(2x-1)}{(2x-1)(x+1)} = \frac{(A-B)+(A+2B)x}{2x^2+x-1}. \end{aligned}$$

Equating the coefficients in the numerators yields the 2 equations

$$A - B = 2, \quad A + 2B = 1.$$

Subtracting the second equation from the first tells us that $-3B = 1$, so $B = -1/3$. Then the first equation tells us that $A = 2 - (1/3) = 5/3$. So we have

$$f(x) = \frac{5/3}{2x-1} - \frac{1/3}{x+1} = -\frac{5/3}{1-2x} - \frac{1/3}{1+x}.$$

The coefficient of x^r in $1/(1-x)$ is 1, so

- the coefficient of x^r in $1/(1-2x)$ is 2^r (by replacing x with $2x$), and
- the coefficient of x^r in $1/(1+x)$ is $(-1)^r$ (by replacing x with $-x$)

Therefore, the coefficient of x^r in the generating function $f(x)$ is

$$-\frac{5}{3}(2^r) - \frac{1}{3}(-1)^r.$$

Solutions to Exercise 8.8.

1) Let $C(x) = \displaystyle\sum_{n=0}^{\infty} c_n x^n$ be the generating function of $\{c_n\}$. Then

$$\begin{aligned} C(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + \cdots \\ xC(x) &= \qquad c_0x + c_1x^2 + c_2x^3 + c_3x^4 + \cdots \\ x^2C(x) &= \qquad\qquad c_0x^2 + c_1x^3 + c_2x^4 + \cdots \end{aligned}$$

so

$$\begin{aligned} (1 - x - 2x^2)C(x) &= C(x) - xC(x) - 2x^2C(x) \\ &= c_0 + (c_1 - c_0)x + \sum_{n=2}^{\infty}(c_n - c_{n-1} - 2c_{n-2})x^n \\ &= c_0 + (c_1 - c_0)x, \end{aligned}$$

since (by the recurrence relation) we have $c_n - c_{n-1} - 2c_{n-2} = 0$ for $n \geq 2$. Therefore

$$C(x) = \frac{c_0 + (c_1 - c_0)x}{1 - x - 2x^2}.$$

Since $c_0 = 2$ and $c_1 = 0$, this means

$$C(x) = \frac{2 + (0-2)x}{1 - x - 2x^2} = \frac{2 - 2x}{(1+x)(1-2x)}.$$

We now use partial fractions. Write

$$\frac{2-2x}{(1+x)(1-2x)} = \frac{A}{1+x} + \frac{B}{1-2x} = \frac{A(1-2x) + B(1+x)}{(1+x)(1-2x)} = \frac{(A+B) + (B-2A)x}{(1+x)(1-2x)}.$$

Equating the coefficients in the numerators yields the equations

$$2 = A + B, \qquad -2 = B - 2A.$$

Subtracting the second equation from the first tells us that

$$2 - (-2) = (A + B) - (B - 2A) = 3A,$$

so $A = 4/3$. Then the second equation tells us that

$$B = 2A - 2 = 2(4/3) - 2 = 2/3.$$

So

$$C(x) = \frac{2-2x}{(1+x)(1-2x)} = \frac{A}{1+x} + \frac{B}{1-2x} = \frac{4/3}{1+x} + \frac{2/3}{1-2x} = \frac{4}{3}\left(\frac{1}{1+x}\right) + \frac{2}{3}\left(\frac{1}{1-2x}\right).$$

From the generalized binomial theorem, we know:

- The coefficient of x^n in $\dfrac{1}{1+x} = (1+x)^{-1}$ is

$$\binom{-1}{n} = (-1)^n \binom{1+n-1}{n} = (-1)^n \binom{n}{n} = (-1)^n.$$

- The coefficient of x^n in $\dfrac{1}{1-2x} = (1-2x)^{-1}$ is

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

Therefore c_n, the coefficient of x^n in $C(x)$, is $\dfrac{4}{3}(-1)^n + \dfrac{2}{3} \cdot 2^n$.

3) Let $E(x) = \displaystyle\sum_{n=0}^{\infty} e_n x^n$ be the generating function of $\{e_n\}$. Then

$$\begin{aligned}
E(x) &= e_0 + e_1 x + e_2 x^2 + e_3 x^3 + e_4 x^4 + \cdots \\
xE(x) &= \qquad e_0 x + e_1 x^2 + e_2 x^3 + e_3 x^4 + \cdots \\
\frac{1}{1-x} &= 1 \;\;+\;\; x + \;\; x^2 + \;\; x^3 + \;\; x^4 + \cdots
\end{aligned}$$

so

$$\begin{aligned}(1-3x)E(x)+\frac{2}{1-x} &= E(x)-3xE(x)+2\cdot\frac{1}{1-x}\\ &= (e_0+2)+\sum_{n=1}^{\infty}(e_n-3e_{n-1}+2)x^n\\ &= (e_0+2),\end{aligned}$$

since (by the recurrence relation) we have $e_n-3e_{n-1}+2=0$ for $n\geq 1$. Therefore

$$E(x)=\frac{(e_0+2)-\dfrac{2}{1-x}}{1-3x}=\frac{(e_0+2)(1-x)-2}{(1-3x)(1-x)}.$$

Since $e_0=2$, this means

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

We now use partial fractions. Write

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

Equating the coefficients in the numerators yields the equations

$$2=A+B,\qquad -4=-(A+3B).$$

Adding the two equations tells us that $2-4=(A+B)-(A+3B)=-2B$, so $B=1$. Then the first equation tells us that $A=2-B=2-1=1$. So

$$E(x)=\frac{2-4x}{(1-3x)(1-x)}=\frac{A}{1-3x}+\frac{B}{1-x}=\frac{1}{1-3x}+\frac{1}{1-x}.$$

From the generalized binomial theorem, we know that the coefficient of x^n in $\frac{1}{1-3x}$ is 3^n, and the coefficient of x^n in $\frac{1}{1-x}$ is 1. Therefore e_n, the coefficient of x^n in $E(x)$, is 3^n+1.

Solutions for Chapter 9

Solutions to Exercise 9.3.

2) To prove Proposition 9.2 requires strong induction, since the recursive relation calls on two previous terms. Thus, two base cases are required.

3) The formula from Proposition 9.2 gives

$$\begin{aligned}D_5 &= 5!\left(\frac{(-1)^0}{0!}+\frac{(-1)^1}{1!}+\frac{(-1)^2}{2!}+\frac{(-1)^3}{3!}+\frac{(-1)^4}{4!}+\frac{(-1)^5}{5!}\right)\\ &= 120\left(1-1+\frac{1}{2}-\frac{1}{6}+\frac{1}{24}-\frac{1}{120}\right)\\ &= 60-20+5-1=44.\end{aligned}$$

4) The initial conditions are $D_1=0$ and $D_2=1$. The recursive relation $D_n=(n-1)(D_{n-1}+D_{n-2})$ for $n\geq 3$ gives $D_3=2(D_2+D_1)=2(1+0)=2$.

Now

$$D_4=3(D_3+D_2)=3(2+1)=9,$$

and

$$D_5 = 4(D_4 + D_3) = 4(9 + 2) = 4(11) = 44.$$

Solutions to Exercise 9.5.

1) **PROOF.** Base case: $n = 0$. We have $c_0 = 1$ (by definition) and $1 > 0$, so $c_0 > 0$.

Inductive step: We begin with the inductive hypothesis. We will require strong induction. Let $k \geq 0$ be arbitrary, and suppose that the inequality holds for every j with $0 \leq j \leq k$; that is, assume that for every such j, $c_j > 0$.

Now we want to deduce that $c_{k+1} > 0$. Using the recursive relation, we have

$$c_{k+1} = \sum_{i=0}^{k} c_i c_{(k+1)-i-1} = \sum_{i=0}^{k} c_i c_{k-i}.$$

Using the inductive hypothesis, we have $c_j > 0$ for every j such that $0 \leq j \leq k$. Putting these together gives that c_{k+1} is a sum of $k + 1$ terms where each term has the form $c_i c_{k-i}$ with $0 \leq i \leq k$. Since $0 \leq k - i \leq k$, we see that $c_i > 0$ and $c_{k-i} > 0$ so that $c_i c_{k-i} > 0$. Hence

$$c_{k+1} = \sum_{i=0}^{k} c_i c_{k-i} > 0.$$

This completes the proof of the inductive step.

By the Principle of Mathematical Induction, $c_n > 0$ for every $n \geq 0$. □

Solutions to Exercise 9.11.

1)

$$\begin{aligned} B_4 = \sum_{k=1}^{4} \binom{3}{k-1} B_{4-k} &= \binom{3}{0} B_3 + \binom{3}{1} B_2 + \binom{3}{2} B_1 + \binom{3}{3} B_0 \\ &= 5 + 3(2) + 3(1) + 1(1) = 15. \end{aligned}$$

3) If $b_i = (i + 1)!/2$ then the expanded exponential generating function for this sequence is

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

This is

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

Solutions for Chapter 10

Solutions to Exercise 10.10.

1) Since there are 8 rows on a chessboard, and $17 > 2(8)$, the Generalised Pigeonhole Principle says that there must be at least $2 + 1 = 3$ rooks that are all in the same row of the board. Choose such a row, and call it Row A. Note that Row A contains at most 8 rooks.

   There are at least $17 - 8 = 9$ rooks that are not in Row A. Since there are 7 other rows on the chessboard, and $9 > 1(7)$, the Pigeonhole Principle says that there must be at least $1 + 1 = 2$ rooks that are in the same row, from amongst the other rows of the board. Choose such a row, and call it Row B. Note that Row B also contains at most 8 rooks.

   There is at least $17 - 8 - 8 = 1$ rook remaining, so there must be a rook somewhere on the board that is in neither Row A nor Row B. Choose such a rook, Rook 1, and call the row that it is in Row C. Since there are at least 2 rooks in Row B, at least one of them must not be in the same column as Rook 1. Choose such a rook, Rook 2. Since there are at least 3 rooks in Row A, at least one of them must not be in the same column as either Rook 1 or Rook 2. Choose such a rook, and call it Rook 3. Now Rooks 1, 2, and 3 do not threaten each other, so fulfil the requirements of the problem.

3) We use the even more generalised pigeonhole principle with $n - 1 = 15$ for the adults, and $n_2 = 23$ for the children (and $m = 2$ categories: adults and children). The principle tells us that as long as at least

$$n_1 + n_2 - m + 1 = 15 + 23 - 2 + 1 = 37$$

   people are approached, he will have enough people to carry his art in the parade.

Solutions to Exercise 10.18.

2) Of the basic pieces of information that we need to complete a Venn diagram, one has not been given to us: the number of Kevin's apps that are free and require internet access. Fortunately, we can use inclusion-exclusion to work this out from the others. We use F to represent the set of free apps; G to represent the games, and I to represent the apps that require internet. Then we have been told:

$$|F| = 78, |I| = 124, |G| = 101, |F \cap G| = 58, |G \cap I| = 62, |F \cap G \cap I| = 48, |F \cup G \cup I| = 165.$$

   Using inclusion-exclusion, we have

$$165 = 78 + 124 + 101 - 58 - 62 - |F \cap I| + 48,$$

   so

$$|F \cap I| = 78 + 124 + 101 - 58 - 62 + 48 - 165 = 66.$$

   The value we have been asked for is

$$|F \cap I \cap \overline{G}| = |F \cap I| - |F \cap I \cap G| = 66 - 48 = 18.$$

3) The number of integers between 1 and 60 that are divisible by 2 is $60/2 = 30$. Call the set of these integers A. The number of integers between 1 and 60 that are divisible by 3 is $60/3 = 20$. Call the set of these integers B. The number of integers between 1 and 60 that is divisible by 5 is $60/5 = 12$. Call the set of these integers C. Then $|A \cap B|$ is the number of integers between 1 and 60 that are divisible by 2 and 3; that is, the number that are divisible by 6. This is $60/6 = 10$. Similarly, $|A \cap C|$ is the number of integers between 1 and 60 that are divisible by 2 and 5; that is, the number that are divisible by 10. This is $60/10 = 6$. Also, $|B \cap C|$ is the number of integers between 1 and 60 that are divisible by 3 and 5; that is, the number that are divisible by 15. This

is $60/15 = 4$. Finally, $|A \cap B \cap C|$ is the number of integers between 1 and 60 that are divisible by 2, 3, and 5; that is, the number that are divisible by 30. This is $60/30 = 2$.

We have been asked for $|A \cup B \cup C|$. Using inclusion-exclusion, we see that the answer is $30 + 20 + 12 - 10 - 6 - 4 + 2 = 44$.

Solutions for Chapter 11

Solutions to Exercise 11.11.

1) a) The only edge incident with a is e_1, so the valency of a is 1.

b) The only edge incident with b is e_2, so the valency of b is 1.

c) The edges incident with c are e_1, e_3, and e_4, so the valency of c is 3.

d) The edges incident with d are e_2, e_3, and e_5, so the valency of d is 3.

e) The edges incident with e are e_4, e_5, and e_6, so the valency of e is 3.

Since $e_6 = \{e, e\}$ is a loop, the graph is **not** simple. There is no isolated vertex, because no vertex has valency 0. The only neighbour of a is c, and the only edge incident with a is e_1.

3) a) The edges incident with a are e_1 and e_2, so the valency of a is 2.

b) The edges incident with b are e_1 and e_3, so the valency of b is 2.

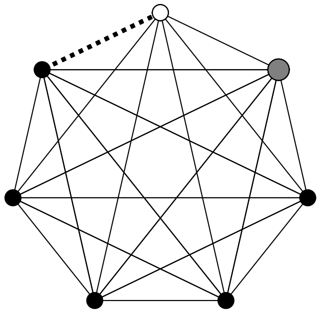
c) The edges incident with c are e_2 and e_3, so the valency of c is 2.

d) No edges are incident with d, so the valency of d is 0.

There are no loops or multiple edges, so the graph is simple. The graph does have an isolated vertex, namely, d (because the valency of d is 0). The neighbours of a are b and c, and the edges incident with a are e_1 and e_2, as was already mentioned above.

Solutions to Exercise 11.22.

3) In the following picture, the dotted line represents the edge we will delete. If we then delete the white vertex, the graph that remains is complete. If instead we then delete the large grey vertex (which is the next one clockwise from the white vertex), the remaining graph will not be complete, since the white vertex is only adjacent to four of the five black vertices.



4) **PROOF.** Let G be a graph with e edges.

Base case: $e = 0$. Since G has no edges, every vertex has valency 0. So the number of vertices of odd valency is 0, which is even.

Inductive step: We begin with the inductive hypothesis. Fix $e \geq 0$, and assume that every graph with e edges has an even number of vertices of odd valency.

Now we want to deduce that every graph with $e + 1$ edges has an even number of vertices of odd valency. Let H be an arbitrary graph with $e + 1$ edges. Choose one edge f (there is one since $e + 1 \geq 1$), and call its endvertices u and v. Let $H' = H \setminus \{f\}$.

Notice that H' has $e + 1 - 1 = e$ edges, so our induction hypothesis applies to H'. Therefore, H' has an even number of vertices of odd valency. Call this number $2m$, where $m \in \mathbb{Z}$.

Observe that the valency of every vertex of H is the same as its valency in H' if the vertex is not u or v, and is one greater than its valency in H' if the vertex is either u or v. Consider the three possible cases: u and v both have even valency in H'; u and v both have odd valency in H'; or exactly one of u and v has even valency in H'.

If u and v both have even valency in H', then they both have odd valency in H, so the number of vertices of odd valency in H must be $2m + 2$, which is even.

If u and v both have odd valency in H', then they both have even valency in H, so the number of vertices of odd valency in H must be $2m - 2$, which is even.

If exactly one of u and v has even valency in H', then exactly one of u and v will have even valency in H (the other one, since the valency of each of u and v goes up by 1). So the number of vertices of odd valency in H must be $2m$ (even though one of the specific vertices of odd valency has changed between u and v), which is even.

In all cases, H has an even number of vertices of odd valency. This completes the proof of the inductive step.

By the Principle of Mathematical Induction, every graph with at least 0 edges has an even number of vertices of odd valency. □

Solutions to Exercise 11.29.

1) The graphs are not isomorphic, because the only vertex of valency 1 in G (namely, c) is adjacent to a vertex of valency 3 (namely d), but the only vertex of valency 1 in H (namely, z) is adjacent only to a vertex of valency 1 (namely, y).

   Here is a more complete proof. Suppose $\varphi\colon G \to H$ is an isomorphism. (This will lead to a contradiction.) We must have

$$d_H\big(\varphi(c)\big) = d_G(c) = 1.$$

   (This principle was pointed out in the proof of Proposition 11.26(3).) The only vertex of valency 1 in H is z, so this implies that $\varphi(c) = z$.

   Now, since $d \sim c$, we must have $\varphi(d) \sim \varphi(c)$. Since $\varphi(c) = z$, and the only neighbour of z is y, this implies $\varphi(d) = y$. So

$$d_H(y) = d_H\big(\varphi(d)\big) = d_G(d).$$

   However, $d_H(y) = 2$ and $d_G(d) = 3$, so $d_H(y) \neq d_G(d)$. This is a contradiction.

3) There is no vertex of valency 0 in G_1, but A is a vertex of valency 0 in G_2. Therefore G_1 and G_2 do not have the same degree sequence, so they are not isomorphic.

Solutions to Exercise 11.30.

2) Of the five vertex labels, we can choose any two to join with an edge. Thus, the number of labeled graphs on five vertices with one edge is $\binom{5}{2} = 10$.

3) Notice that there are $\binom{5}{2} = 10$ total edges possible in a graph on 5 vertices. Thus, the number of labeled graphs on 5 vertices with 3 edges is the number of ways of choosing 3 of these 10 labeled edges. So there are $\binom{10}{3} = 120$ labeled graphs on 5 vertices that have 3 edges.

Similarly, there are $\binom{10}{4} = 210$ labeled graphs on 5 vertices that have 4 edges. Thus, in total there are $120 + 210 = 330$ labeled graphs on 5 vertices that have 3 or 4 edges.

Solutions for Chapter 12

Solutions to Exercise 12.6.

1) **PROOF.** We prove, by induction on n, that if $n \geq 1$, and G is any digraph with n vertices that has no loops or multiarcs, then

$$|A(G)| = \sum_{v \in V(G)} d^+_G(v) = \sum_{v \in V(G)} d^-_G(v).$$

Base case: $n = 1$. Let G be a digraph with no loops or multiarcs, and with only one vertex v_1. Then there are no arcs in G, so $|A(G)| = 0 = d^+_G(v_1) = d^-_G(v_1)$. So the desired conclusion is true when $n = 1$.

We now establish the induction step. Assume that $n \geq 1$, the formula holds for every digraph with n vertices that has no loops or multiarcs, and G is a digraph with $n+1$ vertices that has no loops or multiarcs.

Pick an arbitrary vertex u of G. Let

- N^+ be the set of outneighbours of u, and N^- the set of inneighbours of u,
- $s = |N^+| = d^+_G(u)$ be the number of arcs that begin at u,
- $t = |N^-| = d^-_G(u)$ be the number of arcs that end at u, and
- G' be the digraph obtained from G by deleting u and its $s + t$ incident arcs.

Note that:

- $V(G') = V(G) \smallsetminus \{u\}$, so G' has n vertices.
- $|A(G')| = |A(G)| - s - t$.
- For $v \in V(G') \smallsetminus N^-$, we have $d^+_{G'}(v) = d^+_G(v)$ (because the outneighbours of v in G' are exactly the same as the outneighbours of v in G).
- For $v \in N^-$, we have $d^+_{G'}(v) = d^+_G(v) - 1$ (because u is counted as an outneighbour of v in G, but it is not in G' so it cannot be counted as an outneighbour in G').
- Similar statements hold with N^- replaced by N^+.

Hence

$$\begin{aligned}
\sum_{v \in V(G)} d^+_G(v) &= \sum_{v \in V(G) \smallsetminus (N^- \cup \{u\})} d^+_G(v) + \sum_{v \in N^-} d^+_G(v) + \sum_{v \in \{u\}} d^+_G(v) \\
&= \sum_{v \in V(G) \smallsetminus (N^- \cup \{u\})} d^+_{G'}(v) + \sum_{v \in N^-} \big(d^+_{G'}(v) + 1 \big) + d^+_G(u) \\
&= \left(\sum_{v \in V(G) \smallsetminus N^- \cup \{u\}} d^+_{G'}(v) + \sum_{v \in N^-} d^+_{G'}(v) \right) + |N^-| + d^+_G(u) \\
&= \sum_{v \in V(G')} d^+_{G'}(v) + t + s \\
&= |A(G')| + s + t \qquad \text{(induction hypothesis)} \\
&= |A(G)|.
\end{aligned}$$

Similarly, we can argue that $\displaystyle\sum_{v \in V(G)} d^-G(v) = |A(G)|$. This completes the inductive step and the proof. □

3) Beginning at the top and working clockwise, label the vertices of the digraph a, b, c, d, and e. Then:
   - a has outvalency 2 and invalency 1;
   - b has outvalency 2 and invalency 2;
   - c has outvalency 1 and invalency 2;
   - d has outvalency 2 and invalency 2;
   - e has outvalency 1 and invalency 1.

Solutions to Exercise 12.12.

2) This graph is connected. To see this, note that $(a, j, g, v, e, d, i, h, c, b)$ is a walk that passes through all of the vertices of G, so it is possible to walk from a to any other vertex. Therefore, the connected component that contains a is $V(G) = \{a, b, c, d, e, f, g, h, i, j\}$.

   There are several walks of length 5 from a to f. One example is (a, g, a, j, g, f).

3) This graph is **not** connected. To see this, note that there are no edges from any vertex in $\{a, d, e, f, g, j\}$ to any vertex in $\{b, c, h, i\}$. Indeed the connected component that contains a is $\{a, d, e, f, g, j\}$. (The walk (a, d, e, f, g, j) passes through all of these vertices, but none of these vertices are adjacent to any vertex that is not in the subset.)

   There are several walks of length 3 from a to d. One example is (a, d, a, d).

Solutions to Exercise 12.22.

1) (a) There are many paths of length 3. One example is (a, b, c, h).

   (b) (b, c, f, b) is a cycle of length 3.

   (c) (a, b, c, b) is neither a path nor a cycle. It is not a path because the vertices are not all distinct. (Namely, the vertex b occurs twice.) It is not a cycle, because the first vertex (namely, a) is not the same as the final vertex (namely, b).

3) **PROOF.** Let $(u = u_1, u_2, \ldots, v = u_k, u)$ be a cycle of G in which u and v appear as consecutive vertices. Let $G' = G \setminus \{uv\}$.

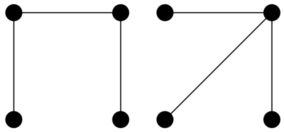
   Let x and y be arbitrary vertices of G. Since G is connected, there is a walk $(x = x_1, x_2, \ldots, x_m = y)$ from x to y in G. If this walk does not contain the edge uv then it is also a walk in G'. If it does contain the edge uv, then we can find some i with $1 \leq i \leq m-1$ such that either $x_i = u$ and $x_{i+1} = v$, or vice versa. For every such i, replace the pair (x_i, x_{i+1}) in the walk by either $(u = u_1, u_2, \ldots, v = u_k)$ or $(v = u_k, u_{k-1}, \ldots, u = u_1)$ (as appropriate, depending on whether $x_i = u$ or $x_i = v$). The result is a walk from x to y that does not use the edge uv, so is in G'. Since x and y were arbitrary vertices of G', for any two vertices x and y of G' there is an $x - y$ walk, so by definition, G' is connected. □

Solutions to Exercise 12.28.

1) **PROOF.** Let T be a tree, and let v be a leaf of T. Consider $T \setminus \{v\}$. Certainly it cannot have any cycles, since T has no cycles. Let x and y be arbitrary vertices of $T \setminus \{v\}$. Since T is connected, there is an $x - y$ walk in T, so by Proposition 12.16, there is an $x - y$ path in T. Since v is a leaf of T, if an $x - y$ walk uses the vertex v then the neighbour of v would have to come both before and after v in the walk, since

v has only one neighbour, so such a walk would not be a path. Thus, the $x - y$ path cannot use the vertex v, so it is still a path in $T \setminus \{v\}$. Since x and y were arbitrary vertices, this shows that $T \setminus \{v\}$ is connected. This completes the proof. □

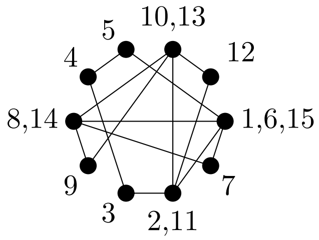
3) The two nonisomorphic unlabeled trees on 4 vertices are:



Solutions for Chapter 13

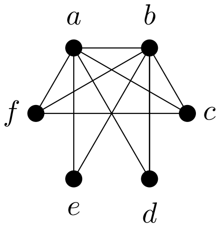
Solutions to Exercise 13.6.

1) This graph has Euler tours, because it is connected and all vertices have even valency. One Euler tour is $(d, f, g, j, a, d, e, i, h, b, f, c, b, i, d)$. The following figure numbers the vertices $1, 2, 3, \ldots$ in the order they are visited.



Solutions to Exercise 13.19.

2) (a) In the closure, we can join a to b; we can join a to c; and we can join b to f. This completes the closure, shown below. It is not easy to see from this whether or not the graph has a Hamilton cycle. In fact, it does not.



(b) The closure of this graph is K_6. We can easily see from this that the graph does have a Hamilton cycle.
(To see that the closure is K_6, observe that every vertex of the graph has valency at least 2. Thus, the two vertices of valency 4 can be joined to each of their non-neighbours. After doing so, every vertex has valency at least 3, so every vertex can be joined to every other vertex.)

3) Let G be the graph that has been shown here. Using the notation of Theorem 13.9, let $S = \{a, f\}$. Then $|S| = 2$, but $G \setminus S$ has 3 connected components: $\{b, e\}$, $\{c, h\}$, and $\{d, g\}$. Since $3 > 2$, G cannot have a Hamilton cycle.

Solutions for Chapter 14

Solutions to Exercise 14.18.

1) **PROOF.** Trees are bipartite (they have no cycles at all, so certainly do not have any cycles of odd length), so Theorem 14.17 tells us that they are class one. □

2) **PROOF.** The proof is by contradiction: suppose n is odd, and the cycle

$$C_n = (v_0, v_1, \ldots, v_n = v_0)$$

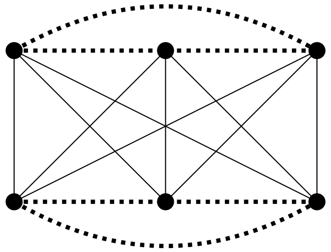
is class one. Since every vertex of C_n has valency two, this means that the graph has a proper edge-colouring that uses only 2 colours. Let us call the colours red and blue.

Assume, without loss of generality, that the edge v_0v_1 is red. The edge v_1v_2 cannot be the same colour as v_0v_1 (because they are both incident to v_1), so v_1v_2 must be blue. The edge v_2v_3 cannot be the same colour as v_1v_2 (because they are both incident to v_2), so v_2v_3 must be red. Continuing in this way, we see (by induction on k) that v_kv_{k+1} is red whenever k is even, and it is blue whenever k is odd. (That is, the two colours must alternate red,blue,red,blue,red,blue,... as we go around the cycle.)

In particular, since n is odd, we know that $n-1$ is even, so this means that the edge $v_{n-1}v_n$ is red. However, we have $v_n = v_0$ so the edges $v_{n-1}v_n$ and v_0v_1 are both incident to the vertex v_0), so they cannot be the same colour. The contradicts the fact that both edges are red. □

Solutions to Exercise 14.24.

1) The following 2-colouring of the edges of K_6 has no solid triangle and no dotted K_4 (because the solid edges form $K_{3,3}$, which has no cycles of odd length, and each connected component of the dotted graph is only K_3):



3) **PROOF.** We prove this by induction on $k+\ell$. The base case is when $k+\ell=2$ (so $k=\ell=1$). Then

$$R(k,\ell) = R(1,1) = 1 < 4 = 2^{1+1} = 2^{k+\ell}.$$

So the inequality is valid in the base case.

For the induction step, assume $k+\ell \geq 2$, and that $R(k',\ell') \leq 2^{k'+\ell'}$, whenever $k'+\ell' < k+\ell$. Since $R(k,\ell) = R(\ell,k)$, we may assume $k \leq \ell$ (by interchanging k and ℓ, if necessary). If $k=1$, then

$$R(k,\ell) = R(1,\ell) = 1 = 2^0 < 2^{k+\ell}.$$

Therefore, we may assume $2 \leq k \leq \ell$. Since $(k-1)+\ell < k+\ell$ and $k+(\ell-1) < k+\ell$, the induction hypothesis tells us that

$$R(k-1,\ell) \leq 2^{(k-1)+\ell} \quad \text{and} \quad R(k,\ell-1) \leq 2^{k+(\ell-1)}.$$

Therefore

$$\begin{aligned}
R(k,\ell) &\le R(k-1,\ell)+R(k,\ell-1) && \text{(Proposition 14.23)}\\
&\le 2^{(k-1)+\ell}+2^{k+(\ell-1)} && \text{(induction hypothesis)}\\
&= 2^{k+\ell-1}+2^{k+\ell-1}\\
&= 2\cdot 2^{k+\ell-1}\\
&= 2^{k+\ell}.
\end{aligned}$$

This completes the proof. □

4) Since $R(k,\ell) \le R(k',\ell')$ whenever $k \le k'$ and $\ell \le \ell'$, we have

$$40 \le R(3,10) \le R(3,11).$$

Also, since $R(k,\ell) \le R(k-1,\ell)+R(k,\ell-1)$ and $R(2,\ell)=\ell$, we have

$$R(3,11) \le R(3-1,11)+R(3,11-1) = R(2,11)+R(3,10) \le 11+42 = 53.$$

So $40 \le R(3,11) \le 53$.

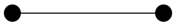
Solutions to Exercise 14.26.

2) **PROOF.** We assume that $N-1 > (c+1)(n-1)$. Consider an arbitrary colouring of the edges of K_N with $c+1$ colours. Fix a vertex v. Since v has $N-1 > (n-1)(c+1)$ incident edges, the generalised pigeonhole principle tells us that there must be some set of at least n edges incident with v that are all coloured with the same colour, say colour i. Look at the induced subgraph of K_N on the n other endpoints of these edges. If any edge xy of this induced subgraph is coloured with colour i, then all of the edges of the triangle $\{v,x,y\}$ have been coloured with colour i, so K_N has a monochromatic triangle.

If on the other hand no edge of the induced subgraph has been coloured with colour i, then the induced subgraph is a K_n whose edges have been coloured with the remaining c colours. By hypothesis, every such colouring has a monochromatic triangle. This completes the proof. □

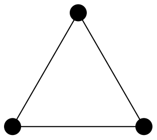
Solutions to Exercise 14.28.

1) We are looking for the smallest value of n such that every edge-colouring of K_n with dotted, dashed, and solid lines has either a dashed K_2 or a dotted K_2 or a solid triangle. The following colouring shows that $R(2,2,3) > 2$:



However, $R(2,2,3)=3$. This is because if any edges are dotted or dashed, then there is a dotted or dashed K_2; if no edges are dotted or dashed, then every edge is solid, so there is a solid K_3.

2) We will show that $R(2,4)=4$. We are looking for the smallest value of n such that every edge-colouring of K_n with dashed or solid lines has either a dashed K_2 or a solid K_4. The following colouring shows that $R(2,4) > 3$;



However, in K_4 if any edge is dashed, then there is a dashed K_2, while if no edges are dashed, then there is a solid K_4.

Solutions to Exercise 14.43.

2) **PROOF.** We will proceed by induction on n.

Base case: $n = 1$. Then K_1 is the graph with one vertex and no edges, and $\chi(K_1) = 1$. Thus, when $n = 1$ we have $\chi(K_n) = n$.

Induction step: We begin with the induction hypothesis. Let $k \geq 1$ be arbitrary, and assume that $\chi(K_k) = k$, so we can properly colour K_k using k colours, and k colours are required to do so.

Now consider the graph K_{k+1}. Let v be an arbitrary vertex of this graph. By our induction hypothesis, $\chi(K_{k+1} \setminus \{v\}) = k$. Thus, any proper colouring of K_{k+1} must use at least k colours on the vertices other than v. It is not possible to colour v with any of these k colours, since v is adjacent to all of the other vertices, so has a neighbour that is coloured with each of these k colours. Therefore, $\chi(K_{k+1}) \geq k + 1$. In fact, since v is the only vertex not yet coloured by these k colours, it is clear that $k + 1$ colours suffice to colour the graph: we colour v with a new colour, which is the $k + 1$st colour. This will certainly be a proper colouring of K_{k+1}. Thus, $\chi(K_{k+1}) = k + 1$, completing the induction step.

By the Principle of Mathematical Induction, $\chi(K_n) = n$ for every $n \geq 1$. □

4) The fact that G contains a subgraph isomorphic to K_i implies that $\chi(G) \geq i$. The fact that $\Delta(G) \leq j$ implies that

$$\chi(G) \leq \Delta(G) + 1 \leq j + 1.$$

So $4 \leq i \leq \chi(G) \leq j + 1 \leq 7$.

If we also know that G is connected and is neither a complete graph nor a cycle of odd length, then $\chi(G) \leq \Delta(G) \leq j$, so $4 \leq i \leq \chi(G) \leq j \leq 6$ in this case.

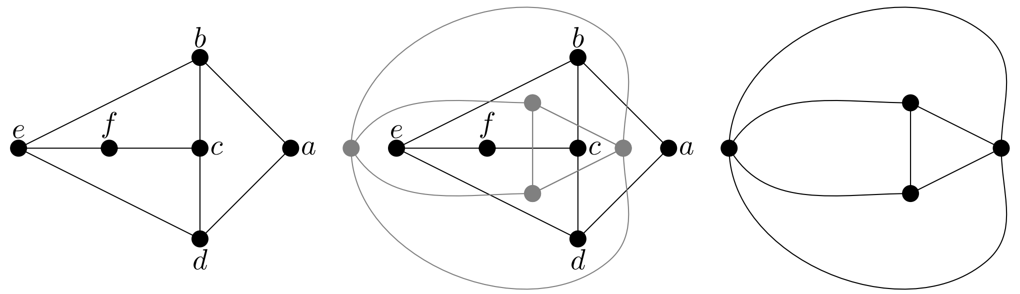
Solutions for Chapter 15

Solutions to Exercise 15.16.

1) **PROOF.** Let G be a graph with a nonplanar subgraph H. Suppose (towards a contradiction) that G is planar. Find a planar embedding of G, and delete vertices and/or edges (as appropriate) to reach the subgraph H. No edges that do not share an endvertex have points in common in the embedding of G, and edges that do share an endvertex have no other points in common. This property is not changed by deleting vertices and/or edges, so our result is a planar embedding of H. But this is impossible, since H is nonplanar. The contradiction shows that G must be planar.

Since K_5 is a subgraph of K_n for every $n \geq 6$ and K_5 is nonplanar by Theorem 15.3, this shows that K_n is nonplanar for every $n \geq 6$. □

3) We show a planar embedding of the graph, the planar embedding with the dual graph shown in grey, and the dual graph.



Solutions to Exercise 15.26.

1) We will prove that for any planar embedding of a disconnected planar graph with exactly two connected components, $|V| - |E| + |F| = 3$.

PROOF. We will prove this formula by induction on the number of faces of the embedding. Let G be a planar embedding of a graph with exactly two connected components.

Base case: If $|F| = 1$ then G cannot have any cycles (otherwise the interior and exterior of the cycle would be 2 distinct faces). So G must consist of two connected graphs that have no cycles, i.e., two trees, T_1 and T_2. By Theorem 12.27 we know that we must have $|E(T_1)| = |V(T_1)| - 1$ and $E(T_2) = V(T_2) - 1$, so

$$|V| - |E| + |F| = |V(T_1)| + |V(T_2)| - (|V(T_1)| - 1) - (|V(T_2) - 1) + 1 = 3.$$

Inductive step: We begin by stating our inductive hypothesis. Let $k \geq 1$ be arbitrary, and assume that for any planar embedding of a graph that has exactly two connected components, such that the embedding has k faces, $|V| - |E| + |F| = 3$.

Let G be a planar embedding of a graph that has exactly two connected components, such that the component has $k + 1 \geq 2$ faces. Since forests have only one face, G must have a cycle in at least one of its components. Choose any edge e that is in a cycle of G, and let $H = G \setminus \{e\}$. Clearly, we have

$$|E(H)| = |E(G)| - 1$$

and $|V(H)| = |V(G)|$. Also,

$$|F(H)| = |F(G)| - 1 = k$$

since the edge e being part of a cycle must separate two faces of G, which are united into one face of H. Furthermore, since e was in a cycle and G has two connected components, by an argument similar to that given in Proposition 12.21 H has two connected components, and H has a planar embedding induced by the planar embedding of G. Therefore our inductive hypothesis applies to H, so

$$\begin{aligned} 2 &= |V(H)| - |E(H)| + |F(H)| \\ &= |V(G)| - (|E(G) - 1) + (|F(G)| - 1) \\ &= |V(G)| - |E(G)| + |F(G)| = 3 \end{aligned}$$

This completes the inductive step.

By the Principle of Mathematical Induction, $|V| - |E| + |F| = 3$ for any planar embedding of graph that has exactly two connected components. □

4) The value for $|V| - |E| + |F|$ on a torus is 0. For example, consider the graph on 5 vertices consisting of two cycles of length 3 that meet at a vertex. Draw this graph on a torus so that one cycle goes through the hole in the middle, and one cycle goes around the outside edge of the torus. This embedding has one face, since the first cycle cuts the torus into something resembling a cylinder, and the second cuts the cylinder into a rectangle. There are 5 vertices and 6 edges, so $|V| - |E| + |F| = 5 - 6 + 1 = 0$, as claimed.

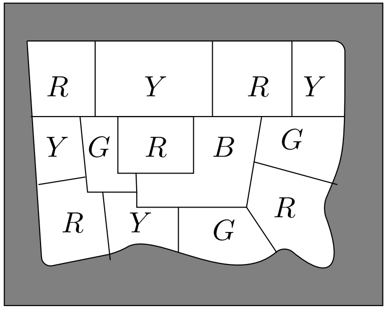
Solutions to Exercise 15.34.

1) First, notice that since G is cubic, every vertex has valency 3, which is odd. Therefore, by Corollary 11.21, G must have an even number of vertices.

This means that the number of vertices in the Hamilton cycle, and the number of edges in the Hamilton cycle (which are equal) are both even. Thus, we can colour the edges of the Hamilton cycle with 2 colours, say blue and red, alternating between the two colours all the way around the cycle.

Since the graph is cubic, each vertex is now incident to exactly one edge that has not yet been coloured. Therefore, we can colour all of the remaining edges with a single colour – green, say. Thus, we have properly 3-edge-coloured G. Since $\Delta(G) = 3$, this means that G is a class one graph.

2) We use the letters R, G, B, and Y to represent the four colours. The exterior face (which appears grey in the picture) will be assigned the colour B.



Solutions for Chapter 16

Solutions to Exercise 16.3.

1) **PROOF.** Let L be an $n \times n$ Latin square whose entries come from a set N of cardinality n, and let L' be the result of exchanging row i with row j.

Let $k \in \{1, \ldots, n\}$ be arbitrary, and consider column k of L'. Its entries are exactly the same as the entries of column k of L, except that the ith entry has been exchanged with the jth entry. Since every element of N appears exactly once in column k of L, it also appears exactly once in column k of L' (although possibly in a different position). Since k was arbitrary, every element of N appears exactly once in each column of L'.

Now consider row k of L'. If $k \neq i, j$, then this row is exactly the same as row k of L. Since every element of N appears exactly once in row k of L, it also appears exactly once (and in the same position even) in row k of L'. If $k = i$ or $k = j$, then row k of L' is the same as some other row (the jth or ith row, respectively) of L. Since every element of N appears exactly once in that row of L, it also appears exactly once in row k of L'.

Thus, L' satisfies the definition of a Latin square. □

2) There are three different ways to complete the square:

$$\begin{array}{cccc} 1 & 3 & 4 & 2 \\ 2 & 1 & 3 & 4 \\ 4 & 2 & 1 & 3 \\ 3 & 4 & 2 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3^{.} \\ 2 & 4 & 3 & 1 \end{array}$$

So the completion is not unique.

Solutions to Exercise 16.12.

2) As explained in the first paragraph of the proof of Theorem 16.7, we may assume the first row is $1, 2, 3, 4$.

Now, we use the idea that is explained in the second paragraph of the proof of Theorem 16.7. For any position in a row after the first row, the entry in our new Latin square cannot be the same as the entry in this position of either of the two given squares (because, for any j, the ordered pair (j, j) has already appeared in the top row of the given square and our new square), and it also cannot be the same as the entry in the first row of the column. This eliminates three possibilities for the entry in this position, so there is only one possibility left. Putting this remaining entry into each position yields the following Latin square, which must be the one that was requested:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}$$

3)

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \end{array}$$

Solutions to Exercise 16.18.

2) This collection has no system of distinct representatives, because the five sets A_2, A_3, A_4, A_5, and A_6 have union $A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6 = \{v, w, x, y\}$, which has cardinality 4.

4) This collection does have a system of distinct representatives: x, y, and z, for A_1, A_2, and A_3 (respectively).

Solutions to Exercise 16.25.

1) Adam, Ella, Jusin, and Bryant are only friends that have visited either England, Scotland, Ireland, France, or Italy. Therefore, she has only 4 friends to choose from to answer the questions for these 5 countries. Since the number of friends is less than the number of countries, she cannot choose a different friend for each of these countries.

2) No, this cannot be completed to a 4×4 Latin square:

- The third entry in the third row must be 1, because 2, 3, and 4 already appear in either the third row or the third column.

- The last entry in the third row must also be 1, because 2, 3, and 4 already appear in either the third row or the last column.

So we cannot complete the third row: we are forced to have 1 appear twice in this row, but that is not allowed.

Hall's Marriage Theorem does not apply to this situation, because, as we have seen, the third column and fourth column must both choose their entry for the third row from the set $\{1\}$, which has less than two elements. (Theorem 16.20 does not apply because the partial Latin square does not consist only of complete rows — it has a row that has only been partially filled in.)

Solutions for Chapter 17

Solutions to Exercise 17.13.

1) Numerically, this property is easy to verify from the proof of Theorem 17.11, which tells us that if b is the number of blocks, then $b = \dfrac{\lambda v(v-1)}{k(k-1)}$, so (dividing both sides by 2 and multiplying through by $k(k-1)$) we have $b\dbinom{k}{2} = \lambda\dbinom{v}{2}$.

   The correspondence is due to the colouring explained in Theorem 17.10.

2) We are given that $v = 16$, $k = 6$, and $\lambda = 3$.

   From the formula $r(k-1) = \lambda(v-1)$, we see that
$$r = \frac{\lambda(v-1)}{k-1} = \frac{3(16-1)}{6-1} = 9,$$
   which means that each point is in 9 blocks.

   Now, from the formula $bk = vr$, we have
$$b = \frac{vr}{k} = \frac{16 \cdot 9}{6} = 24.$$
   This means that the design has 24 blocks.

Solutions to Exercise 17.20.

1) **PROOF.** Clearly the complement of a design will still have v varieties. (It will also have b blocks, since each of its blocks comes from one block of the original design.)

   From a block B of size k, the corresponding block of the complementary design will have the $v-k$ elements of $V \setminus B$.

   We need to count how many times any given pair of varieties appear together in a block of the complementary design. Two varieties appear together in a block of the complementary design if and only if neither of them was in the corresponding block of the original design. Each of the two varieties appeared in r blocks of the original design, and they appear together in λ blocks of the original design. We can now use inclusion-exclusion to count the number of blocks in which at least one of the two varieties appears: $r + r - \lambda = 2r - \lambda$. Thus, the number of blocks in which neither of them appears is $b - (2r - \lambda) = b - 2r + \lambda$, as claimed. Since this count in no way depended on the choice of our two varieties, the complement is indeed a design, as every pair of varieties appear together in some block $b - 2r + \lambda$ times. □

3) The set $\{1, 3, 7\}$ gives the differences ± 2, ± 4, and ± 6, while the set $\{1, 6, 13\}$ gives the differences ± 5, ± 7, and ± 12. So we need to find two sets that contain the differences ± 1, ± 3, ± 8, ± 9, ± 10, and ± 11.

   The sets $\{1, 2, 11\}$ and $\{1, 4, 12\}$ work.

Solutions to Exercise 17.26.

1) Many examples are possible (but they may be hard to find). For example, let

$$v = 16, \;\; k = 6, \;\text{ and }\; \lambda = 1.$$

Then

$$\lambda\frac{v-1}{k-1} = 1 \cdot \frac{16-1}{6-1} = 3$$

and

$$\lambda\frac{v(v-1)}{k(k-1)} = 1 \cdot \frac{16(16-1)}{6(6-1)} = \frac{16 \cdot 15}{6 \cdot 5} = 8$$

are integers, so the conditions in Theorem 17.11 are satisfied.

From the formula $r(k-1) = \lambda(v-1)$, we see that

$$r = \frac{\lambda(v-1)}{k-1} = \frac{1 \cdot (16-1)}{6-1} = 3.$$

Then, from the formula $bk = vr$, we have

$$b = \frac{vr}{k} = \frac{16 \cdot 3}{6} = 8.$$

Therefore $b = 8 < 16 = v$, so Fisher's Inequality is not satisfied.

Since Fisher's Inequality is not satisfied, there is no BIBD with these parameters.

2) It is shown just before the proof of Fisher's Inequality that Fisher's Inequality is equivalent to $\lambda(v-1) \geq k(k-1)$. Since $\lambda = 1$ and $k = 20$, this means

$$1 \cdot (v-1) \geq 20(20-1) = 380,$$

so $v \geq 380 + 1 = 381$. Therefore, v must be at least 381 to satisfy Fisher's Inequality.

Since

$$\lambda\frac{v-1}{k-1} = 1 \cdot \frac{381-1}{20-1} = \frac{380}{19} = 20$$

and

$$\lambda\frac{v(v-1)}{k(k-1)} = 1 \cdot \frac{381(381-1)}{20(20-1)} = \frac{381(380)}{380} = 381$$

are integers, the conditions in Theorem 17.11 are also satisfied. So 381 is the smallest value for v that satisfies all three conditions.

Solutions for Chapter 18

Solutions to Exercise 18.12.

2) Since $v = 39 = 6 \cdot 6 + 3 \equiv 3 \pmod 6$, the proof of Theorem 18.8 tells us that we should use a Latin square constructed in Lemma 18.4. Since $v/3 = 39/3 = 13$, the Latin square is of order $n = 13$, so the first sentence of the proof of Lemma 18.4 tells us that the first row of the Latin square is

$$1 \quad \frac{13+3}{2} \quad 2 \quad \frac{13+5}{2} \quad 3 \quad \frac{13+7}{2} \quad 4 \quad \cdots \quad 13 \quad \frac{13+1}{2}.$$

In other words, the first row is

$$1 \quad 8 \quad 2 \quad 9 \quad 3 \quad 10 \quad 4 \quad 11 \quad 5 \quad 12 \quad 6 \quad 13 \quad 7.$$

Then the second sentence of the proof of Lemma 18.4 tells us that the rest of the rows are obtained by shifting to the left. So the Latin square is

$$\begin{array}{rrrrrrrrrrrrr}
1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 \\
8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 \\
2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 \\
9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 \\
3 & 10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 \\
10 & 4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 \\
4 & 11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 \\
11 & 5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 \\
5 & 12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 \\
12 & 6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 \\
6 & 13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 \\
13 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 \\
7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 & 12 & 6 & 13
\end{array}$$

4) No, it is not a Kirkman system.

We will call $\{u_1, \ldots, u_5\}$ the u-girls; $\{v_1, \ldots, v_5\}$ the v-girls; and $\{w_1, \ldots, w_5\}$ the w-girls. Of the 35 blocks that we obtained through the construction, 5 have one u-girl, one v-girl, and one w-girl; the other 30 have either two u-girls with a v-girl, two v-girls with a w-girl, or two w-girls with a u-girl.

A Kirkman system requires us to divide the blocks into 7 groups of 5 blocks such that each girl appears exactly once in each group of blocks. Since there should be 7 groups of 5 blocks, but there are only 5 blocks that have a u-girl, a v-girl, and a w-girl, there must be at least one group of blocks (in fact, at least two) that has no block consisting of a u-girl, a v-girl, and a w-girl.

Consider such a group of 5 blocks. We must have all 5 of the u-girls. If no block contained more than one u-girl, then in order to get all 5 u-girls we would have to choose only blocks that have two w-girls and a u-girl. However, this would mean that we had 10 w-girls and no v-girls, which is not allowed. So we must choose at least one block that has two u-girls and a v-girl. Repeating the same argument with v or w taking the place of u, we see that we must also choose at least one block that has two v-girls and a w-girl, and at least one block that has two w-girls and a u-girl. Since we are only choosing 5 blocks but there are these three classes of blocks, there must be some class of blocks of which we only choose one.

Without loss of generality, suppose that we only choose one of the blocks that has two u-girls and a w-girl. In order to have all 5 of the u-girls, we must choose three blocks that have two w-girls and a u-girl. But this means that we have six w-girls, which is not allowed.

Therefore, there is no way to partition the blocks of this design into seven groups of five blocks so that every girl appears exactly once in each group.

Solutions to Exercise 18.19.

2) We must have $b\binom{k}{t} = \lambda\binom{v}{t} = \binom{15}{t}$.

Since we are not including any trivial $t-(v,t,1)$ design, we have $t \geq 2$, $3 \leq k \leq 14$, and $t < k$.

Now

$$\frac{15!}{t!(15-t)!} = b\frac{k!}{t!(k-t)!},$$

which means that

$$\frac{15 \cdot 14 \cdots (16-t)}{k(k-1)\cdots(k+1-t)}$$

is an integer.

Furthermore, we have $\binom{k-1}{t-1}$ divides $\binom{14}{t-1}$, so that $\frac{(k-1)!}{(k-t)!}$ divides $\frac{14!}{(15-t)!}$. In other words,

$$\frac{14!(k-t)!}{(15-t)!(k-1)!} = \frac{14 \cdot 13 \cdots (16-t)}{(k-1)(k-2)\cdots(k+1-t)}$$

is an integer. If we call this integer y, combining this with the previous paragraph tells us that k is a divisor of $15y$. We can also further work with the algebra to obtain

$$y = \frac{14 \cdot 13 \cdots k}{(15-t)(14-t)\cdots(k+1-t)}.$$

When $k = 14$, this gives $y = 14/(15-t)$. Since k divides $15y$ and k is coprime to 15, we must have k divides y. But then $y/14 = 1/(15-t)$ is an integer, implying $t = 14$. This contradicts $t < k$. Thus $k = 14$ cannot arise.

When $k = 13$ this gives $y = \frac{14 \cdot 13}{(15-t)(14-t)}$. Since k divides $15y$ and k is coprime to 15, we must have k divides y. But then $\frac{y}{13} = \frac{14}{(15-t)(14-t)}$ is an integer. Since $t < k = 13$, we have $14 - t \geq 2$, but no two consecutive integers each of which is at least 2 are both divisors of 14, a contradiction. Thus $k = 13$ cannot arise.

When $k = 12$, this gives

$$y = \frac{14 \cdot 13 \cdot 12}{(15-t)(14-t)(13-t)}.$$

Now k dividing $15y$ implies that

$$\frac{15 \cdot 14 \cdot 13}{(15-t)(14-t)(13-t)}$$

is an integer. Since the numerator is not a multiple of 2^2, the denominator cannot be either, leaving only the possibilities $t = 4, 8$. Since the numerator is not a multiple of 3^2, the denominator cannot be either, which eliminates $t = 4$. When $t = 8$, the numerator of y is not a multiple of 5, but the denominator is, so this is also impossible. Thus $k = 12$ cannot arise.

When $k = 11$ this gives

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11}{(15-t)(14-t)(13-t)(12-t)}.$$

Since k divides $15y$ and k is coprime to 15, we must have k divides y. But then

$$\frac{y}{11} = \frac{14 \cdot 13 \cdot 12}{(15-t)(14-t)(13-t)(12-t)}$$

is an integer. Since the numerator is not a multiple of 5, the four consecutive numbers that are the factors of the denominator must be 6 through 9 (since $t \geq 2$, they cannot be 11 through 14, and since $t < 11$ they cannot be 1 through 4). Thus, we must have $t = 6$. But then the numerator is not divisible by 3^2, while the denominator is divisible by 3^3, contradicting $y/11$ being an integer. Thus $k = 11$ is not possible.

When $k = 10$, this gives

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{(15-t)(14-t)(13-t)(12-t)(11-t)}.$$

Now k dividing $15y$ implies that

$$\frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11}{(15-t)(14-t)(13-t)(12-t)(11-t)}$$

is an integer. Since the numerator is not a multiple of 2^4, the denominator cannot be either. In particular, 8 cannot be one of the factors that appears in the denominator (since some other even factor would appear with it), nor can 2, 4, and 6 all be factors that appear in the denominator. Also, the numerator is not divisible by 3^3, so we cannot have $11 - t = 9$. This leaves $t = 8$ as the only possibility. However, the numerator of y is not divisible by 3^2, so $t = 8$ is also not possible. Thus $k = 10$ is not possible.

When $k = 9$, we see that

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)}.$$

So k dividing $15y$ gives

$$\frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)}$$

being an integer. Since the numerator is not divisible by 2^5, the denominator cannot be either. In particular, 8 cannot appear as one of the factors in the denominator (or two other numbers divisible by 2 would also appear as factors), so the only possibility is $t = 8$. However, if we take $k = 9$, $t = 8$, and $i = 2$, the necessary condition is $\binom{7}{6} = 7$ divides $\binom{13}{6}$, which is not true. Thus, $k = 9$ is not possible.

When $k = 8$, we calculate

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)}.$$

Since k divides $15y$ and k is coprime to 15, we must have k divides y. But then

$$\frac{y}{8} = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)}.$$

Since the consecutive factors in the denominator include 8 and at least two other even numbers, this implies that the numerator should also be a multiple of 2^5, but it is not. Thus $k = 8$ is not possible.

When $k = 7$ we see that

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)(8-t)}.$$

Since the consecutive factors in the denominator include 6 and 9, if they also include another multiple of 3 then the numerator must be divisible by 3^4, but it is not. This leaves the possibility that $t = 4$ so the factors in the denominator are 4 through 11, but this is divisible by 5^2, which the numerator is not. Thus, $k = 7$ is not possible.

If $k = 6$ then

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)(8-t)(7-t)}.$$

So k dividing $15y$ gives

$$\frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)(8-t)(7-t)}$$

being an integer. The numerator is not divisible by 2^8, so the denominator cannot be either; in particular it cannot include as factors all of the even integers from 4 through 10 as well as one other. This leaves the possibilities $t = 2$ and $t = 4$. If $t = 2$ then $y = 14/5$ which is not an integer, and similarly if $t = 4$ then we have $y = \dfrac{14 \cdot 13 \cdot 12}{5 \cdot 4 \cdot 3}$ which is not an integer. So $k = 6$ is not possible.

If $k = 5$ then

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)(8-t)(7-t)(6-t)}.$$

The numerator is not divisible by 2^9, so the denominator cannot be either; in particular, the denominator cannot include all of 4, 6, 8, 10, and 12 as factors in the product. This leaves only the possibility $t = 4$. If $k = 5$ and $t = 4$ then $i = 0$ gives $\binom{5}{4} = 5$ divides $\binom{15}{4} = 1365$ which is true; $i = 1$ gives $\binom{4}{3} = 4$ divides $\binom{14}{3} = 364$ which is true; $i = 2$ gives $\binom{3}{2} = 3$ divides $\binom{13}{2} = 78$, which is true; $i = 3$ gives $\binom{2}{1} = 2$ divides $\binom{12}{1} = 12$, which is true. Thus a $4-(15,5,1)$ design could exist, but this is the only possibility with $k = 5$.

When $k = 4$ we have

$$y = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{(15-t)(14-t)(13-t)(12-t)(11-t)(10-t)(9-t)(8-t)(7-t)(6-t)(5-t)}.$$

The denominator includes 3, 6, 9, and 12, so is divisible by 3^5, but the numerator is not. Thus, $k = 4$ is not possible.

If $k = 3$ then $2 \leq t < k$ implies $t = 2$. We know these parameters are possible, as these are the parameters of a Steiner triple system.

Thus, the only possible values of k and $t \geq 2$ for which nontrivial t-designs might exist with $v = 15$ and $\lambda = 1$ are $k = 5$ and $t = 4$: a $4-(15,5,1)$ design, or $k = 3$ and $t = 2$: a $(15,3,1)$ Steiner triple system.

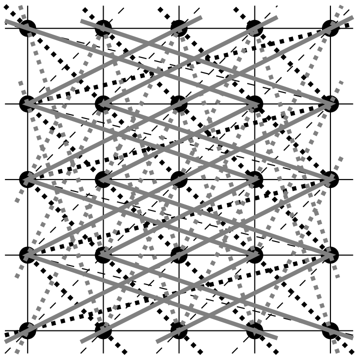
3) If a $3-(16,6,1)$ design exists then we have $bk = vr$ and $b\binom{k}{t} = \lambda\binom{v}{t}$. The second equation gives $b\binom{6}{3} = \binom{16}{3}$, so $b = 28$, so it would have 28 blocks. Now $bk = vr$ gives $28 \cdot 6 = 16r$. This has no integral solution, so such a design is not possible.

Solutions to Exercise 18.28.

1) **PROOF.** Let L, M, and N be lines of an affine plane such that L is parallel to both M and N; that is, no point lies on both L and M or on both L and N. Let p be an arbitrary point on M. Since L and M are parallel, p does not lie on L. By the parallel postulate, there is a unique line through p that is parallel to L; this line is M. Therefore N cannot contain p. Since our choice of p on M was arbitrary, no point of M can also lie on N, so M and N are parallel. □

3) A finite affine plane of order 19 has $19^2 = 361$ points, and $19(19+1) = 380$ lines.

5) Without colours it is difficult to effectively draw this plane so that the parallel classes can be clearly seen. We will use solid vertical lines; solid horizontal lines; dashed lines; dotted lines; solid grey lines; and dotted grey lines to represent the six parallel classes of lines, but some of these may be difficult to distinguish. Note that the lines that are neither vertical nor horizontal will "turn corners" or zig-zag to join their sets of 5 points.



We obtain the following 4 MOLS of order 5 from this affine plane, by using the vertical and horizontal lines to create the coordinates. To make things easier to see, we will have the positions in the Latin squares correspond visually to the positions in the 5 by 5 array of points that we have drawn, so the top-left entry in the Latin squares will come from the top-left point of the array, etc. We will number the lines in each parallel class so as to ensure that the entries in the top row of each square are 1, 2, 3, 4, and 5, in that order. The first square corresponds to the dashed lines; the second to the dotted lines; the third to the solid grey lines, and the fourth to the dashed grey lines.

$$\begin{array}{ccccc} 1&2&3&4&5\\ 2&3&4&5&1\\ 3&4&5&1&2\\ 4&5&1&2&3\\ 5&1&2&3&4 \end{array}\quad \begin{array}{ccccc} 1&2&3&4&5\\ 5&1&2&3&4\\ 4&5&1&2&3\\ 3&4&5&1&2\\ 2&3&4&5&1 \end{array}\quad \begin{array}{ccccc} 1&2&3&4&5\\ 3&4&5&1&2\\ 5&1&2&3&4\\ 2&3&4&5&1\\ 4&5&1&2&3 \end{array}\quad \begin{array}{ccccc} 1&2&3&4&5\\ 4&5&1&2&3\\ 2&3&4&5&1\\ 5&1&2&3&4\\ 3&4&5&1&2 \end{array}$$

Solutions to Exercise 18.32.

1) No, not every design with $\lambda = 1$ is is a projective plane. The condition $\lambda = 1$ ensures that every two points have a unique line that is incident with both of them. However, there is no requirement in a design that every two blocks have a nonempty intersection. (If every two blocks do have a nonempty intersection, then the condition $\lambda = 1$ does force the intersection to have exactly one point.) The condition that there exist four points such that no three are incident with a single line can also fail, but only in trivial or complete situations.

3) From Theorem 16.10, we know that there are $p - 1$ MOLS of order p whenever p is prime. This implies that there is a projective plane that has $p + 1$ points on each line whenever p is prime.

4) Since there are not 5 MOLS of order 6 (as we saw in Euler's problem), there is no projective plane that has 7 points on each line.

Solutions for Chapter 19

Solutions to Exercise 19.5. The only string with an odd number of 1s is 10101, so it is not an allowable message, but all of the others are allowed.

Solutions to Exercise 19.12.

1) The only such word is "math."

3) There are many possibilities, such as "$\underline{\text{b}}$at$\underline{\text{s}}$," "$\underline{\text{g}}$a$\underline{\text{s}}$h," and "ma$\underline{\text{ny}}$."

5) We have answered this in each solution given above.

Solutions to Exercise 19.13.

2) **PROOF.** Let x and y be words of the same length. We have $d(x, y) = 0$ if and only if x and y differ in no positions. This means that x must have the same entry as y in every position, which means $x = y$. □

4) **PROOF.** Let x, y, and z be words of the same length. Suppose that $d(x, z) = k$, so that x and z differ in k positions. Suppose that $d(x, y) = i$, so y differs from x in i positions. If $i \geq k$ then since $d(y, z) \geq 0$ by part (1), we have $d(x, z) \leq d(x, y) + d(y, z)$. Otherwise, there must be some list of at least $k - i$ positions in which x differs from z but does not differ from y. In each of these positions, since y has the same entry as x, y must have a different entry than z. Therefore $d(y, z) \geq k - i$. Now $d(x, y) + d(y, z) \geq i + k - i = k = d(x, z)$, completing the proof.

Solutions to Exercise 19.17.

3) The minimum distance is 2. To see this, first note that $d(01011, \underline{10}011) = 2$, so the minimum distance is no more than 2. Since each of the nonzero codewords has exactly three 1s, its distance from 00000 is 3, and its distance to any other nonzero codeword is greater than 1, because changing a single bit will change the number of 1's. So the minimum distance is at least 2.

Solutions to Exercise 19.20.

2) (a) The code can detect 5 errors, but not 6 (because the number of errors detected must be less than the minimum distance).

   (b) The code can correct 2 errors (because $2 \times 2 < 6$, but $2 \times 3 \not< 6$).

Solutions to Exercise 19.27.

1) Since

$$G = \begin{bmatrix} I_k \\ A \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix},$$

we have

$$G \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \qquad G \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad G \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

This means that 0101 encodes as 010111, 0010 encodes as 001000, and 0010 encodes as 111001.

Solutions to Exercise 19.32.

Since $G = \begin{bmatrix} I_k \\ A \end{bmatrix}$, and the given matrix G has 4 columns, we must have $k = 4$, so $I_k = I_4$ has 4 rows. Therefore, A is all but the first 4 rows of G, which means

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Since A is a 3×4, matrix, we have $r = 3$, so the parity-check matrix is

$$P = [A\ I_r] = [A\ I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Solutions to Exercise 19.39.

2) (a) Yes, all six columns of the parity-check matrix are different from each other (and none of them are all 0), so Theorem 19.36 tells us that the code can correct all single-bit errors.

(b) Let P be the given parity-check matrix. Then:

- ∘ $P \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$ This is the 5th column of P, so changing the 5th bit corrects the error. The received word 001001 decodes as 0010$\underline{1}$1.

- ∘ $P \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$ This is 0, so there is no error. The received word 110011 decodes as 110011.

- ○ $P \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}.$ This is the 2nd column of P, so changing the 2nd bit corrects the error. The received word 000110 decodes as $0\underline{1}0110$.

Solutions to Exercise 19.42.

1) There are $2^5 - 1 = 31$ different nonzero 5-bit strings. Of these 31 strings, 5 of them have only one 1. Thus, there are $31 - 5 = 26$ different nonzero strings with at least two 1s. Therefore, we can make a 5×24 matrix A, such that the columns of A are 24 different binary column vectors with at least two 1s in each column (because there are 26 different possible columns to choose from, and we need only 24 of them). The columns of the resulting parity-check matrix $P = [A\ I_5]$ are all nonzero and distinct, so Theorem 19.36 tells us that the resulting binary linear code can correct every single-digit error.

   Furthermore, since P is 5×24, we know that $r = 5$ and $k = 24$. Since $r = n - k$, this implies $n = k + r = 24 + 5 = 29$. So the code is of type $(n, k) = (29, 24)$, as desired.

3) Suppose P is the the parity-check matrix of a binary linear code of type (n, k) that corrects all single-bit errors, and let $r = n - k$. Then Theorem 19.36 tells us that the columns of P must be distinct (and nonzero). However, P is $r \times n$, and $n = k + r$, so it has $k + r$ columns of length r, and there are only $2^r - 1$ different possible nonzero columns of length r. Therefore, we must have $k + r \leq 2^r - 1$. Conversely, if this inequality is satisfied, then we can construct a $k \times (k + r)$ parity-check matrix whose columns are all distinct and nonzero. Thus, the smallest possible number of check bits is the smallest value of r that satisfies the inequality $k + r \leq 2^r - 1$.

   Thus:

   - $r = 2$ check bits suffice for $k = 1$, because $k + r = 1 + 2 = 3 = 2^2 - 1 = 2^r - 1$.
     (But $r = 1$ check bit does not suffice, because $k + r \geq 1 + 1 = 2 > 2^1 - 1 = 2^r - 1$.)
   - $r = 3$ check bits suffice for $k = 2, 3, 4$, because $k + r \leq 4 + 3 = 7 = 2^3 - 1 = 2^r - 1$.

     (But $r = 2$ check bits do not suffice, because $k + r \geq 2 + 2 = 4 > 2^2 - 1 = 2^r - 1$.)
   - $r = 4$ check bits suffice for $5 \leq k \leq 11$, because $k + r \leq 11 + 4 = 15 = 2^4 - 1 = 2^r - 1$.

     (But $r = 3$ check bits do not suffice, because $k + r \geq 5 + 3 = 8 > 2^3 - 1 = 2^r - 1$.)
   - $r = 5$ check bits suffice for $12 \leq k \leq 20$, because $k + r \leq 20 + 5 = 25 < 31 = 2^5 - 1 = 2^r - 1$.
     (But $r = 4$ check bits do not suffice, because $k + r \geq 12 + 4 = 16 > 2^4 - 1 = 2^r - 1$.)

Solutions to Exercise 19.45.

1) Using Proposition 19.44, we have $v = 10$, $k - 2 = 4$ so that $k = 6$, and $\lambda = 1$. The question is asking us for b. Using $bk(k - 1) = \lambda v(v - 1)$ gives $30b = 90$ so $b = 3$. Such a code will have only 3 words.