Combinatorics

KNU Math 254

Classnotes

Mark Siggers

v. June 15, 2020

These notes are for a third year course in Combinatorics. The course is based on Richard Brualdi's Introductory Combinatorics 5^{th} edition. We refer to this as the text.

Chapter 1

What is Combinatorics?

Combinatorics is about counting. As the name 'combinatorics' seems to suggest, we will count combinations, and their dirty cousin, permutations– we do this in Chapter 2– but we count all sorts of things. The word 'combinatorics' is more a description of how we count, in that we will count structures by counting the ways that we can combine their bits to construct them.

We will count such things as

- solutions to equations/problems, or
- elements of constructed sets, or
- configurations satisfying a certain property.

Typical problems we will encounter are the the following, and their numerous variations:

- How many different pizza's can we make with 3 of 7 possible toppings?
- How many ways can we distribute 10 candies among 4 children?

The first chapter of the text gives several non-trivial examples of standard or typical combinatorical problems. We cover only three of them: sections 1.1, 1.4, and 1.7 of the text, (their numbering will be different in the notes) but students are encouraged to at least look at the others.

1.1 Perfect Covers of Chessboards

An $m \times n$ *chessboard* is simply a rectangle of size $m \times n$ (centimeters, obviously), divided into $m \times n$ unit squares. Often it comes with an attractive colouring as pictured in Figure 1.1, but we might remove this.

A *domino* is a 1×2 rectangle. You can turn it on its side and make a 2×1 rectangle. A *(perfect) cover* of chessboard by dominos is an arrangement of dominos on the chessboard so that the whole

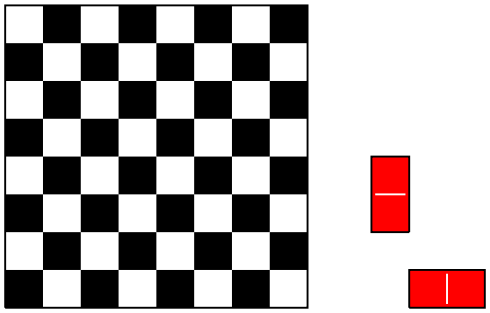


Figure 1.1: A white-black coloured 8×8 chessboard and some dominos

chess board is covered by dominos which no-where overlap. It is easy to see that a 2×2 chessboard can be covered by 2 dominos– and indeed can be coverd by them in two different ways. (If you think it is four or more then you are counting 'flips' of the dominos that I am not.)

Here is a hard problem. Don't do it!

How many ways can you cover an 8×8 chessboard by dominos?

But think about it. Can you get some easy estimates on it? We can. This is somthing we love to do in combinatorics– estimate things.

We can cut an 8×8 chessboard up into 16 squares of dimension 2×2. Lets just count the perfect covers that contain perfect covers of these 16 squares. Each little square can be covered in 2 ways. So there are $2^{16} \approx 10^5$ such covers. So we know there are (easily) more than 10^5 covers of an 8×8 chessboard.

On the other hand, pick any of the 64 squares of the 8×8 chessboard. In a cover, this square can be covered in at most 4 different ways: the domino covering it can also cover the square to its north, south, east or west. If I know 'how' each square is covered, then I know the covering, so there are at most 4^{64} different coverings. We can even refine this argument. I only have to know how the white squares are covered, to know the covering. So there are at most $4^{32} = 2^{64} \approx 10^{19}$ different coverings.

Practice 1.1.1

Some of the white squares are on the edge or in corners so have fewer possible coverings. How much does this reduce your upper bound of the number of different coverings of the 8×8 chessboard?

Where $c(m, n)$ is the number of coverings of an $m \times n$ chessboard by dominos, we have observed that

$$2^{16} \leq c(8, 8) \leq 2^{64}.$$

This is still a big gap. Fischer showed in about 1960 that $c(8, 8) = 12,988,816$,

What can we say about $c(m,n)$ for different values of m and n? Well, it is known, but a bit hard right now. Let's look at the easier question of deciding when $c(m,n)$ is 0. The first step is pretty easy.

Practice 1.1.2

Show that if mn is odd, then $c(m,n) = 0$.

The second step almost as easy.

Practice 1.1.3

Show that if m is even. then whatever $n \geq 1$ is, $c(m,n) > 0$.

Well done Larry. You've proved your first theorem.

Theorem 1.1.1. *An $m \times n$ chessboard has a perfect covering by dominos if and only if mn is even.*

Note

The phrase 'if and only if' is often used in proofs and statements, and often shortened to 'iff'. If you want to prove an 'iff' statement, you usually have two things to prove, as we had above.

What happens now if we change the dimensions of our dominos? For any integer $b \geq 1$ a b-omino is a $1 \times b$ (or $b \times 1$) tile. When does an $m \times n$ chessboard have a cover by b-ominos.

Practice 1.1.4

Show that if an $m \times n$ chessboard has a cover by b-ominos then b divides mn. Show that if b divides m or n, then an $m \times n$ chessboard has a cover by b-ominos. Conclude that if b is prime, then and $m \times n$ chessboard has a cover by b-ominos if and only if b divides mn.

What happens if b is not prime. This is a little bit trickier. Does a 2×3 chessboard have a cover by 6-ominos? Nonesense! Hmm... so what do we conjecture? Lets prove the following.

Theorem 1.1.2. *An $m \times n$ chessboard has a cover by b-ominos iff b divides m or n.*

Proof. We have already proved the 'if' part of the 'if and only if' we have to prove the 'only if': that there is a cover only if b divides m or n. We can assume that there is a cover and show that b divides m or n. Another way to prove this statement is to assume that there is a cover, and that b does not divide m, and then show that b must divide n. This is how we do it.

Let $r = m \mod b$ and $q = m \mod b$. (Recall that $x \mod p$ is the remainder on dividing x by p.) As we have assume that b doesn't divided m, we have that r is not zero. So $1 \leq r \leq b-1$. We have also that $0 \leq q \leq b-1$, and our goal is to show that $q = 0$, as this means that b divides n.

Number the squares in the chessboard, as if they were entries in an matrix, letting $S_{i,j}$ be the i^{th} square from the top and the j^{th} from the left. Colour square $S_{i,j}$ with colour $i + j - 1 \mod b$.

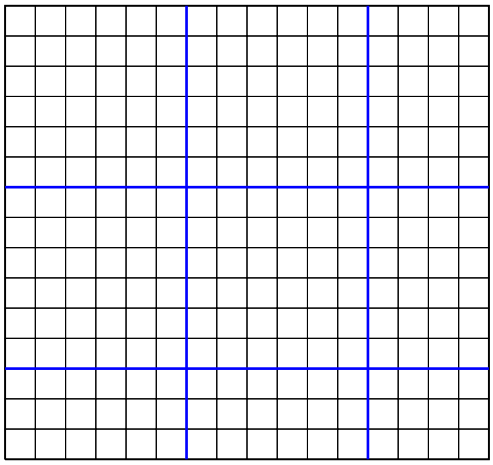


Figure 1.2: Cutting a chessboard into $b \times b$ squares

(Really do it!). Any b-omino in a cover of the chessboard must cover one square of each colour, so if there is a cover then we must have the same number of squares of each colour under this colouring.

Now, divide the chessboard up into rectangles by cutting down the ib^{th} vertical line for each integer $i \in 1, 2, \ldots \lfloor m/b \rfloor$, and cutting across the ib^{th} horizontal line for each $i \in 1, 2, \ldots \lfloor n/b \rfloor$ (see Figure 1.2).

The bigger $b \times b$ squares, and any rectangle with long dimension b has the same number of squares of each colour. So this whole thing has the same number of squares of each colour if and only if that $r \times q$ square in the bottom right does. If $q > 0$ then this square is non-empty. Assume this is true. It has colour r in its top right corner, and from there we can see it has an r-coloured square in every row. But it doesn't have an b-coloured square in its first row, and has at most one in any row. So it contains more r-coloured squares than b-coloured squares. We said this is impossible if there is a covering, so if there is a covering, then $q = 0$, as we wanted to show. □

1.2 The four-colour theorem

See the video on the website.

1.3 Nim

See the video on the website.

Problems from the text

Section 1.8: 2, 3, 5, 20, 25, 28

Chapter 2

Permutations and Combinations

In this chapter, we define sets and count their elements.

Example 2.0.1. Let S be the set of students in this classroom today. Find $|S|$, the cardinality (number of elements) of S.

It's not my fault if you didn't come to class. Use your \$%\$%&# imagination.

2.1 Basic Counting Principles

There are a couple of simple principles we use quite frequently in counting:

- The addition principle.
- The multiplication principle
- The subtraction principle.
- The division principle.

They are as easy as their names suggest. We use all of them to count S and ignore the fact that our use of them may have dubious efficiency for this particular exercise.

The addition principle If we can partition our set S into disjoint subset

$$S = S_1 \cup S_2 \cup \cdots \cup S_n$$

then $S = |S_1| + |S_2| + \cdots + |S_n|$.

Example 2.1.1. We partition S into the set S_F of female students and S_M of male students, and then count each of these. Then $|S| = |S_F| + |S_M|$.

In Chapter 6, we will see the Inclusion-Exclusion principle, a more sophisticated version of the addition principle.

The multiplication principle If the elements of S can be represented as ordered pairs (a, b) where a can be any of m different values and b can be any of n different values, then $|S| = mn$.

Example 2.1.2. You are sitting in 5 rows of 5 people per row, so $|S| = 5 \cdot 5 = 25$.

The subtraction principle If there is some universe X and S is a subset of the universe, then where $\overline{S} = X \setminus S$ is the *complement* of S in X, we have

$$|S| = |X| - |\overline{S}|.$$

Example 2.1.3. The universe X is the set of chairs in this classroom and by the multiplication principle I know there are 25. When I was writing on the board, some of you rascels snuck out, and now there are two empty seats. Using the subtraction principle I know there are $25 - 2 = 23$ occupied seats. There is a one-to-one correspondence between S and the set of occupied seats, so I know $S = 23$.

The division principle If there is some universe X partitioned into m disjoint sets $X = S_1 \cup S_2 \cup \cdots \cup S_m$ of the same size, then $|S_i| = |X|/m$.

Example 2.1.4. The u students in the university are evenly partitioned among the m different combinatorics classes. So $|S| = u/m$.

Okay. We've had fun stretching an example as far as it can go. Try this more typical example.

Practice 2.1.1

How many two digit numbers are made up of two different digits?

2.2 Permutations of Sets

A *permutation* of a set X is an ordering of its elements. (What is an ordering then? A sequence of length $|X|$ such that each element of X occurs exactly once. But examples are easier to understand this.)

Example 2.2.1. Let $[n]$ denote the n-element set $\{1, 2, \ldots, n\}$. There are 6 permutations of [3]:

$$(1, 2, 3), (2, 3, 1), (3, 1, 2), (1, 3, 2), (3, 2, 1), \text{ and } (2, 1, 3).$$

Practice 2.2.1

How many permutations are there of $[n]$?

Well, here is our main counting technique. We build a permutation in steps and count how many ways we could have accomplished each set.

Solution

To build a permutation of $[n]$ we have n steps. In the i^{th} step, we choose the i^{th} element of the permutation.

- For the first step, we can choose any of n elements, so we can complete the step in n ways.
- For the second step, we can choose any element but the one already chosen, so we have $n-1$ ways.
- $n-2$ ways. Et. cetera.

All told we have $n! = n \times n-1 \times n-2 \times \cdots \times 1$ ways to choose a permutation. So there are $n!$ permutations.

An *r-permutation* of a set X is a permutation of r of its elements. Let $P(n,r)$ be the number of r-permutations of an n element set.

Practice 2.2.2

Give formulas for

- $P(3,1)$
- $P(n,1)$
- $P(n,n)$
- $P(n,n-1)$
- $P(n,r)$

Lets look now at some variations on the Permutaion Problem.

Practice 2.2.3

Answer the following:

i. How many three letter words can we make from the letters $\{a, b, c, d, e\}$?

ii. How many without repetition of letters?

iii. How many ways can we arrange 7 men and 3 women in a line so that no two women stand beside each other?

iv. How many ways can we arrange 10 people in a line if Jack and Jill cannot stand beside each other?

v. How many ways can we arrange 10 around a round table?

This last question was asking for the number of *circular permutations* of an n-element set.

Try to prove this.

Theorem 2.2.2. *There are $P(n, r)/r$ circular r-permutations of an n elements set.*

With this we can answer the following questions.

Practice 2.2.4

Do the following.

i. How many ways can we arrange 10 people around a round table, Jack and Jill not sat together?

ii. How many ways can we arrange 5 couples around a round table, so no couples sit together?

iii. How many ways can we arrange 5 couples around a round table if the couples are all sat diametrically opposite?

2.3 Combinations of Sets

Combinations are permutations that don't care about order. An *r-combination* (or *r-subset*) of a set X is a subset of X of cardinality r. Let $C(n, r) = \binom{n}{r}$ denote the number of r-combinations of an n element set.

There are $P(n, r) = \frac{n!}{(n-r)!}$ r-premutations of $[n]$. For each r-combination X of $[n]$, let S_X be the set of r-permutations that are a permutation of X. Then $|S_X| = r!$. By the division principle we have then that

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

It follows from this formula that

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

There is also a very intuitive 'combinatorics' explanation of this identity: the number of ways of choosing a set X of r elements from n is the same as the number of ways of of choosing the $n-r$ elements of its complement $\overline{X}$.

Practice 2.3.1

Give a 'combinatorial' explanation of this identity.

The symbol $\binom{n}{r}$ is called the *binomial co-efficient* as it arises in the 'Binomial Theorem'.

Practice 2.3.2

Fill in the coefficients in the following expansion using binomial coefficients

$$\begin{aligned}(x+1)^4 &= (x+1)(x+1)(x+1)(x+1)\\ &= __x^4 + __x^3 + __x^2 + __x^1 + __\end{aligned}$$

With the same reasoning you used to to this you get the following.

Theorem 2.3.1 (Binomial Theorem)**.** *For any integer $n \geq 0$*

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

Here are some typical questions in which the binomial coefficient arises naturally. Recall that a set of point in the plane is in *general position* if not three points are in a common line.

Practice 2.3.3

Answer these questions:

i. How many triangles are determined by 12 points in general position in the plane?

ii. How many eight letter words can be constructed using the 26 letters of the alphabet if each word contains at least three vowels...

   (a) if no letter can be used more than once?

   (b) if letters can be re-used?

Usually these two different versions of the eight letter word problem are referred to as choosing letters 'with replacement' or 'without replacement'. The picture this envokes is that we have a bucket of 26 letters, and after we choose one, we can replace it in the bucket or not.

Practice 2.3.4

Give 'arithmetic proofs' and 'combinatorial proofs' of the following identities.

i. Pascal's Formula: for all r with $1 \leq r \leq n-1$ we have

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

ii. For $n \geq 0$, we have

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

2.4 Permutations of Multisets

In a practice problem we asked how many 8 letter words we could make 'with' or 'without replacement'. In the case that we are choosing letters with replacement, there is another way of looking at it. *multiset* is like a set (order is not important,) except that elements may be repeated. Choosing letters with replacement can be viewed as choosing them from a multiset containing many copies of each letter.

The multiset $\{a, a, b, b, b, b, c\}$ has cardinalitiy 7, though as a set it would have cardinality 3. The element b occurs with *multiplicity* 4. We can denote this set compactly as

$$\{2 \cdot a, 4 \cdot b, 1 \cdot b\} := \{a, a, b, b, b, b, c\}.$$

Sometimes we will consider an element occuring infinitely many times, and write this as $\infty \cdot a$.

Practice 2.4.1

How many 3-permutations are there of the multiset $\{\infty \cdot a, \infty \cdot b, \infty \cdot c, \infty \cdot d\}$?

Good work, so you showed the following.

Fact 2.4.1. *If S is a multiset containing k distinct elements each with infinite multiplicity, then there are k^r r-permutations of S.*

In fact, you actually showed the following.

Fact 2.4.2. *If S is a multiset containing k distinct elements each with multiplicity at least r, then there are k^r r-permutations of S.*

Practice 2.4.2

How many permutations does the multiset $\{3 \cdot a, 10 \cdot b, 7 \cdot c, 2 \cdot d\}$ have?

Nice! That generalises to the following.

Theorem 2.4.3. *The multiset*

$$\{n_1 \cdot a_1, n_2 \cdot a_2, \ldots n_k \cdot a_k\}$$

has

$$\frac{n!}{n_1!n_2!\ldots n_k!}$$

permutations.

Try this one.

Practice 2.4.3

Santa has 10 (distinct) presents to distribute among the three children. Lucy was good so she gets six of them. Lisa was bad, so she gets only 1, and Eunjoo gets the other three. How many ways can Santa distribute the presents?

Generalise your argument here to show the following. Do you explain the equality? Try to explain it too.

Theorem 2.4.4. *The number of ways to partition n distinct items into sets of sizes $n_1, n_2, \ldots, n_k$ respectively, where $n = \sum n_i$ is*

$$\frac{n!}{n_1!n_2!\ldots n_k!} = \binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdot \ldots \cdot \binom{n-n_1-\cdots-n_{k-1}}{n_k}.$$

2.5 Combinations of Multisets

Combination version now. Here is the typical question. It's the pizza question from our introduction.

Practice 2.5.1

You want to make a fruit basket containing 12 pieces of fruit. You can choose from (any number of identical) apples, mangos, plums, and those awful yellow melons. How many ways can you make up your fruit basket?

What if you want to have at least one of each fruit?

Not as easy, right? But think of it this way. You have to fill 12 positions, line them up, they are not ordered, so you can assume that all the apples come first, then the mangos, et cetera. To decide the numbers of apples, you can choose with 'gap between positions' you change from apples to mangos. You should have argued the proof of the following theorem.

Theorem 2.5.1. *The number of r-subsets of a multiset containing k distinct elements each with infinite multiplicity is*

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

Now. With exactly this idea, you should be able to solve the following problem too.

Practice 2.5.2

What is the number of non-negative integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 = 20?$$

How about of $x_1 + x_2 + x_3 + x_4 \leq 20$?
How about if $x_1, x_2 \geq 1$ and $x_3 \geq 5$?

2.6 Finite Probability

The counting techniques we have looked at allow us to calculate the odds in many a game of chance. We can reframe them in the convenient language of probability.

Practice 2.6.1

An overcoated man in an alley offers you the following chance, if you give him a dollar. You flip a coin three times. If you get all heads or all tails, he gives you three dollars. Should you play?

Solution

Ignoring the overcoat, lets look at this mathematically. You are investing one dollar. There are 8 possible outcomes of the coin flips, and you win in two of them. If you will you get a return of 3 dollars. So your expected return is $3 * 1/4 = 3/4$ dollar. For an investment of 1, a return of 75 cents is an expected loss of 25 cents. It doesn't make sense to play.

Let's formalise this.

An *experiment* $\mathscr{E}$ is a random choice of one outcome from a finite *sample space* (or set) S. (In probability theory, we may talk about different outcomes occuring with different probability, but for us we will assume that every outcome is equally likely, so occurs with probability $p = 1/|S|$.) An *event* E is a subset of S. The *probability* of E is

$$P(E) = \frac{|E|}{|S|}.$$

Lets see a simple example of an experiment.

Practice 2.6.2

In an experiment, you roll two dice. What is the probability of the event E_7 that the dice sum to 7.

Solution

The sample space is the set

$$S = [6] \times [6] = \{(1,1),(1,2),\ldots(6,6)\}$$

of possible rolls. The event is

$$E_7 = \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}.$$

The probability that the dice add up to 7 is thus

$$Prob(E) = \frac{6}{36} = 1/6.$$

Now Poker is a little more tricky then dice. But not much. Recall that a pack of cards consists of 52 cards. There are 13 *ranks*: $A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q$ and K each occuring with each of four *suits*: ♠, ♢, ♣, ♡.

In the game of poker, you build a *hand* of five cards. The player with the highest hand wins. (This is how I play with my daughter, because she doesn't have any money.) The hands, in increasing order are:

- High card: $A♢, 10♣, 9♢, 5♡, 3♠$
- A pair: $5♢, 5♣, J♣, 8♠, 2♣$ (Two cards of the same rank.)
- Two pairs: $5♢, 5♣, 2♠, 2♣, J♣$
- 3-of-a-kind: $5♢, 5♣, 5♠, J♣, 2♣$
- A straight: $9♢, 8♣, 7♠, 6♣, 5♣$
- A flush: $A♢, 10♢, 9♢, 5♢, 3♢$
- A full house: $J♢, J♣, J♠, A♢, A♡$
- 4-of-a-kind: $5♢, 5♣, 5♠, 5♡, A♣$
- Straight Flush: $Q♢, J♢, 10♢, 9♢, 8♢$

The hands are ordered based on the probability of drawing the hand when drawing 5 random cards.

Practice 2.6.3

i. What is the probability of getting one pair (and no better)?

ii. ... a full house.

iii. ... none of these hands.

That was easy right! Maybe the next is a bit more challenging.

Practice 2.6.4

You are playing a version of poker where you can see three of your cards and three of your opponents. She has $6\clubsuit, 8\clubsuit, 10\clubsuit$ and you have $A\diamondsuit, A\clubsuit, A\spadesuit$. What is the probability that you will win?

Problems from the Text

Sect 2.7: 2, 6, 10, 21, 29, 31, 34, 38, 39, 47, 55, 56, 57, 63

Chapter 3

The pigeonhole principle

3.1 Simple form

The following statement is so obvious that it becomes difficult to prove. So we won't, rather we call it a principle and take it as clear. Possibly you would find a proof of it in a fundamental logic/set-theory course.

Fact 3.1.1 (The pigeonhole principle)**.** *If $n+1$ objects are distributed among n boxes, then an least one box contains more that one object.*

Example 3.1.2. There are four Korean surnames, so in a group of five Koreans, at least two have the same surname.

Though the pigeonhole principle is simple, its use can be complicated. Lets not jump in too quick though. The following is a less cheeky, but only marginally more complicated– I'm not telling you how many boxes and pigeons there are, I'm asking you about one of these. (What are the boxes and what are the pigeons?)

Practice 3.1.1

A drawer contains red, green and yellow socks. How many must you choose to be sure that you have at least two of the same colour?

Let's restate the pigeonhole principle now so it looks more like mathematics.

Fact 3.1.3 (Still the pigeonhole principle)**.** *If X and Y are finite sets and f is a function $f : X \to Y$, then the following hold.*

i. If $|X| > |Y|$ then f is not injective*.*

ii. If $|X| = |Y|$ then f is injective iff it is surjective.

Now let's look at some less trivial applications of the Pigeonhole Principle. If you cannot figure this one out, it is Application 3 from the corresponding section of the text. The solution is there. But try it on your own first.

Practice 3.1.2

Given integers $a_1, \ldots, a_m$ show that there are some i, j with $1 \leq i < j \leq m$ for which

$$m | a_i + a_{i+1} + \cdots + a_j.$$

Note: Recall $a|b$ means that a divides b.

What are the pigeons then? What are the boxes? It is maybe not obvious. Here's a hint: m divides the difference of two numbers if they are the same modulo m. So if we can get two sequences with the same remainder modulo m whose difference is a sequence of the form we are looking for, we should be good.

Note: Recall that $a \bmod m$ is the remainder we get when dividing a by m.

The following is Application 4 from Section 3.1 of the text. If you have trouble, look there for the answer.

Practice 3.1.3

A chessmaster plays 132 game over 11 weeks, she plays at least one game per day. Show that these is some number of consecutive days in which she plays exactly 21 games.

Practice 3.1.4

Prove that for any 5 points in an equilateral triangle of side 1 there must be two whose are distance at most 1/2 apart. Hint: Make 4 pigeonholes.

This is Application 6 of the text:

Practice 3.1.5

(The Chinese Remainder Theorem) Let m and n be relatively prime integers (this means their greatest common divisor is 1) and let a and b be non-negative integers with

$$a < m \text{ and } b < n.$$

Show that there exists some $x < mn$ such that $x \mod m = a$ and $x \mod n = b$.

Practice 3.1.6

Show that every rational number p/q has a repeating decimal expansion.

Practice 3.1.7

In a room of 10 people all having ages between 1 and 60, show that some two disjoint sets of the people have the same age sums.

3.2 Pigeonhole Principle: Strong Form

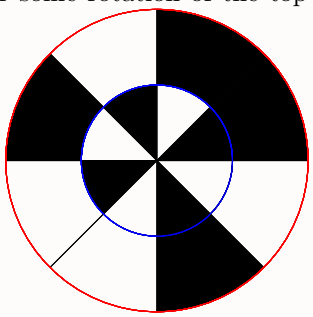
The following more general version of the pigeonhole principle tells can be used to say that amongst a set of values, some value must be at least the average value.

Fact 3.2.1. *Let $q_1, \ldots, q_n$ be positive integers. If $q_1 + \ldots, q_n - n + 1$ items are distibuted among n boxes, then for some $i \in [n]$ the i^{th} box has at least q items.*

Corollary 3.2.2. *If n items are distributed among m boxes, then some box has $\lceil n/m \rceil$ items.*

Practice 3.2.1

Two disks are divided into 8 sections each, and each section is coloured black or white. The larger disk has half of its sections coloured black. Show that for some rotation of the top disk, the two disks have the same colour in at least four sections.



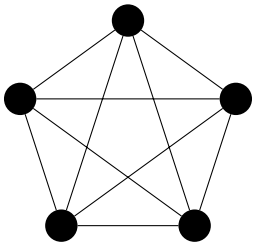
3.3 Ramsey Theory

Consider the following question.

Practice 3.3.1

How many people must there be at a party so that there are 3 people who are mutually acquainted or 3 who are mutually unacquainted?

It is nice to model this with graphs. Recall that a *graph* consists of a set V of *vertices*, and a set E of two element subsets of V, called edges. The graph K_n is the graph on the n vertices $[n]$ with edgeset $E = \{(u, v) \mid u, v \in [n]\}$. The graph K_5 is shown here:



Practice 3.3.2

Find a colouring of the edges of K_5 with the colours red and blue that has no triangle (whose vertices are vertices of the graph), every edge of which is the same colour. Use this to argue that there must be more than 5 people at the party in the previous practice question.

We write $K_p \to (K_m, K_n)$, which we read as K_p 'arrows' K_m and K_n to mean that for every blue-red colouring of the edges of K_p there is a copy of K_m every edge of which is blue, or a copy of K_n every edge of which is red. You have just showed that $K_5 \not\to (K_3, K_3)$. Do the following now to answer our initial question.

Practice 3.3.3

Show that $K_6 \to (K_3, K_3)$.

This proves the easiest non-trivial case of the following theorem of Ramsey.

Theorem 3.3.1. *For all $m, n \geq 2$ there is some integer p such that*

$$K_p \to (K_m, K_n).$$

The *Ramsey number* $r(m, n)$ is the minimum p such that $K_p \to (K_m, K_n)$. You have shown that $r(3, 3) = 6$.

Practice 3.3.4

What is $r(2, n)$?

Apart from $r(3, 3)$ we know very few ramsey numbers exactly. We know:

s, t	3	4	5
3	6		
4	9	18	
5	14	25	$43 - 49$
6	18	$35 - 41$	$58 - 87$
7	23	$49 - 61$	$80 - 143$

We do not even know $r(5, 5)$. It seems like a computer should be able to do it. But to show that it is 43 we would have to show that for each of the $2^{\binom{43}{2}}$ two colourings of the edges of K_{43}, there is a K_5 of one colour. This is a lot of work for a computer. To show that it is not 43, we only have to find one 'good' colouring of K_{43}. Even this is hard.

But we have bounds on the ramsey numbers. The upper bound is easier.

Theorem 3.3.2. *For all $m, n \geq 2$, $r(m, n) \leq \binom{m+n-2}{m-1}$.*

Proof. Our proof is by induction on (m, n). You have already proved the case theorem when either of m or n is 2. Let $m, n \geq 3$ and let G be a graph on $\binom{m+n-2}{m-1}$ vertices. Choose a vertex v_1 and

fix a colouring of the edges of G. Let B be the set of vertices adjacent to v_1 by blue edges and R the vertices adjacent to it by red edges. By the induction hypothesis and Pascals' identity we have that

$$r(m, n-1) + r(m-1, n) = \binom{m+n-3}{m-1} + \binom{m+n-3}{m-2} = \binom{m+n-2}{m-1}$$

which is one more than the number of neighbours that v_1 has, so by the pigeonhole principle we have that $|B|$ is at least $r(m-1, n)$ or that $|R|$ is at least $r(m, n-1)$. Assume the former; then the set B induces a blue K_{m-1}, and so with v_1 we have a blue K_m, or it induces a red K_n, and we are don. The proof in the latter case is the same. □

Setting $m = n$ this gives the following.

Corollary 3.3.3. *For all $n \geq 3$, $r(n, n) \leq 4^n/\sqrt{n}$.*

Proof. Indeed by Stirling's approximation $n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, so

$$r(n, n) \leq \binom{2n-2}{n-1} < \binom{2n}{n} = \frac{(2n)!}{n!n!} < \frac{\sqrt{4\pi n}\left(\frac{2n}{e}\right)^{2n}}{2\pi n\left(\frac{n}{e}\right)^n\left(\frac{n}{e}\right)^n} = \frac{4^n}{\sqrt{n}}.$$

□

Practice 3.3.5

Now, $r = r(m_1, m_2, m_3)$ is the number of vertices we need so that when we three colour the edges of K_r there is a colour i copy of K_{m_i} for some i. Show that $r(3, 3, 3) \leq 17$.

Problems from the Text

Sect 3.4: 5, 10, 12, 15, 20, 27

Chapter 4

Generating Permutations and Combinations

4.1 Generating Permutations

In this section we look at giving lists (that is, orders) of the permutations of a set.

This seems an easy task. I can list the set [3]! of permutations of [3], as

$$123, 132, 213, 231, 312, 321$$

by viewing the permutations as numbers and listing them alphabetically.

I could extend this to an ordering of the permutaitons of any 3-element set simply by associating each element of the set with an element of [3], so I have an ordering of the permutations of the set $\{Adam, Bob, Carol\}$ as

$$(Adam, Bob, Carol), (Adam, Carol, Bob), \ldots, .$$

But there are other ordering that might be better for some purposes. We look at an order in which consecutive permutations in the set differ by the minimum possible difference: they differ only in two places. In the above ordering of S_3 we had 312 following 231. These permutations differ in every coordinate.

Practice 4.1.1

Find an ordering of [3]! in which consecutive permutations have a common digit, (that is, both have an i in the j^{th} digit).

Why might we want to do this? You come up with an idea. A saw a game (called shiri-tori?) on a TV show once where you were given a set of names and you had to order them so that the last letter of the i^{th} word was the same as the first letter of the $i + 1^{th}$ word. How would you do

this if there are a LOT of names. I would get a computer to check all permutations of the names. When the computer is checking each permutation, it can check a lot faster if each permutation is almost the same as the previous one. So there is possibly an application.

Here is the listing of [3]! I asked you for:

$$123, 132, 312, 321, 231, 213.$$

An algorithm to order the permutations of $[n]$

Here is how we make such a listing of $[n]!$. We start recursively from a listing the permutations of [1]!. This is easy:

1

Then we get a listing of [2]! by doubling the above:

1
1

and then inserting a 2 in each space:

1 2
2 1

Now for listing [3]! we need a list of 6 permuations. We triple each line in the above listing of [2]!, and line things up:

1 2
1 2
1 2
2 1
2 1
2 1

Now we run 3 back and forth through each of the slots:

1 2 3
1 3 2
3 1 2
3 2 1
2 3 1
2 1 3

Practice 4.1.2

What is the 10^{th} permutation in the listing of [4]!?

Practice 4.1.3

What is the last permutation in this listing of $[n]!$

A more managable description of the algorithm

Now, nobody wants to write out this whole list for $[6]!$. And even if we did, the way we did it is a bit unwieldy. Lets look at a way to write out the list in a more orderly fashion. Observe with the listing of $[3]!$:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{array}$$

The 3 is always 'moving' from row to row, except when it gets to an end, and then it waits for a step while something else moves. More generally for the listing of $[n]!$, the number n will move ever step except when it gets to an end. When it gets to an end, what moves. Well, usually it is $n-1$, except when, ignoring n, $n-1$ gets to an end. This is the intuition. Let's use some lovely arrows to help us keep track of who is moving, and write out some easy to follow rules.

We start with the permutation $\overleftarrow{1}\,\overleftarrow{2}\,\overleftarrow{3}\ldots\overleftarrow{n}$ in which every number has a left arrow. We will call an integer *mobile* if its arrow is pointing towards a smaller integer. While there is a mobile integer, do the following.

i. Move the largest mobile integer in the direction that its arrow points.

ii. Switch the arrows on any larger integers.

So the listing of $[4]!$ (with arrows) starts as follows:

$$\overleftarrow{1}\,\overleftarrow{2}\,\overleftarrow{3}\,\overleftarrow{4}, \overleftarrow{1}\,\overleftarrow{2}\,\overleftarrow{4}\,\overleftarrow{3}, \overleftarrow{1}\,\overleftarrow{4}\,\overleftarrow{2}\,\overleftarrow{3}, \overleftarrow{4}\,\overleftarrow{1}\,\overleftarrow{2}\,\overleftarrow{3}, \overrightarrow{4}\,\overleftarrow{1}\,\overleftarrow{3}\,\overleftarrow{2}, \overleftarrow{1}\,\overrightarrow{4}\,\overleftarrow{3}\,\overleftarrow{2}, \ldots$$

Practice 4.1.4

Write out the whole listing of $[4]!$ with arrows.

Practice 4.1.5

For each permutation in $[n]!$ there is a unique arrowing that will occur on that permutation if we use this algorithm. In the text, there is an example of an arrowed permutation for $[6]!$: $\overrightarrow{2}\,\overrightarrow{6}\,\overrightarrow{3}\,\overleftarrow{1}\,\overleftarrow{5}\,\overleftarrow{4}$. Is this the correct arrowing for that permuation? (Sure you can list the permutations, but it might be more fun not to. Need a hint? Do the next two practice problems first.)

Practice 4.1.6

What is the 427^{th} permutation of [6]! using the above listing? (I would rather if you didn't list everything, but used some nice reasoning: 'There are $6! = 720$ permutations. In the first 360 of them 1 is before 2,...' Something clever like that is worth a point.)

Practice 4.1.7

We say that the integer i moves at step j of the listing of [6]! if it is the mobile integer we move to get from the j^{th} permuation to the $j + 1^{st}$ permutation. In the listing of [6]!, 6 moves on the j^{th} step for which j? And 4 moves on the j^{th} step for which j?

Choosing a random permutation

To chose a random permutaton $a_1a_2 \dots a_n$ of $[n]$ we can chose a random integer in $[n]$ to be a_1 then a random integer in $[n] \setminus \{a_1\}$ to be a_2, and so on. Another way is the following algorithm, known as the *Knuth shuffle*. For each $k = 1, \dots, n-1$, choose a random position from k to n and switch its entry with the entry in the k position.

Practice 4.1.8

There are exactly $n!$ different 'sets of choices' via the Knuth shuffle. Show that it 'fairly' picks a random permutation by showing that there is a unique way to chose a given permutation. (Think about how it can it yield the permutation 145236?)

4.2 Inversions of Permutations

An *inversion* in an a permutation of $[n]$ is a pair of integers (i, j) such that $i < j$ but j occurs before i.

Example 4.2.1. The permutation 1432 has three inversions: $(3, 4), (2, 4)$ and $(2, 3)$.

Clearly the set of inversions in a permutation define it uniquely, but we can also recognise a permutation by its inversion sequence. Fix a permutation α in $[n]!$. For each $i \in [n]$ let a_i be the number integers greater than it but to its left in α. (That is, the number of inversions that i is the first element of in α).

The *inversion sequence* of α is

$$a_1, a_2, \dots, a_n.$$

Example 4.2.2. The inversion sequence of 1432 is $0, 2, 1, 0$.

Notice that $a_1 \in [0, n-1]$, $a_2 \in [0, n-2]$ and $a_i \in [0, n-i]$ so there are exactly $n \cdot n-1 \cdots = n!$ possible inversion sequences.

Theorem 4.2.3. *There is a one-to-one correspondence between permutations in* $[n]!$ *and permutations sequences– sequences*

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

where $a_i \in [0, n-i]$ *for each* i.

Proof. We have shown that each permutation yields an inversion sequence, and that there are the same number of permutations and inversion sequences, so we have to show that we can get a permuation from its inversion sequence. The text gives two algorithms for this and both are worth reading. We just give the second, as it is easier to implement by hand.

Given an inversion sequence $a_1, a_2, \ldots, a_n$ lay out n spaces. For $i = 1, \ldots, n$ put i in the $(a_i+1)^{th}$ empty spot. To see that 1 is in the right place, we observe that a_1 counts the number of larger elements to its left in the permuations, but all element are larger, so exactly a_1 elements are to the left in the permutation. To see that i is the the right place, recall that a_i is the number of larger elements to its left, and i was placed leaving exactly enough spaces for these.

□

So this gives another ordering of permutations: order the inversion sequences lexicographically (as integers) and use this to order the permuations.

Practice 4.2.1

According to this ordering, what are the first 10 permutations in $[7]!$?

The nice feature of this ordering is that given a permutation, we can use the correspondence to inversion sequences to quickly find the previous or next permtation.

Practice 4.2.2

According to this ordering, what permutations come before and after 4672315 in $[7]!$?

4.3 Generating Combinations

We generated the permutations of a set in various ways. For similar reasons we may want to generate the combinations (subsets) of $[n]$. For subsets there is a one simple ordering that has the very nice property that it is trivial to find the i^{th} subset and to decide where in the order a given subset is, so it is trivial to find the previous or next subset of a given subset.

We let a combination $C \subset [n]$ of $2^{[n]}$ correspond to its *characteristic vector*

$$(v_n, v_{n-1}, \ldots, v_1) \text{ where } v_i = \begin{cases} 0 & \text{if } i \notin C \\ 1 & \text{if } i \in C \end{cases}$$

or the same thing written as a binary string $v_n v_{n-1} \ldots v_1$ or the the integer $\sum_{i=1}^{n} v_i 2^{i-1}$ that this is the binary representation of.

Practice 4.3.1

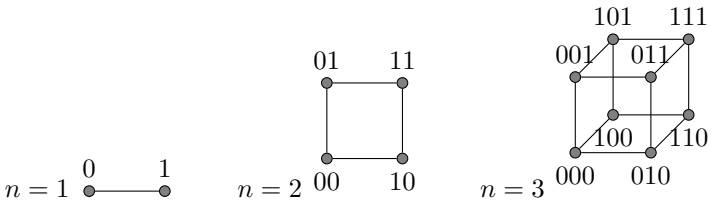
The subset $\{2,3,6\} \subset [8]$ has characteristic vector $(0,0,1,0,0,1,1,0)$ which as a binary string 00100110 is the number $32+4+2=38$. What are the previous and next subsets of $[8]$? What subset comes after $\{1,2,3,4,5,6,7\}$?

Again, it is nice that we can quickly decide what the i^{th} subset of $[n]$ is, but sometimes it is useful to use other orderings in which consecutive subsets are similar.

4.3.1 Gray codes

The *n-dimensional cube*, denoted Q_n is the graph with vertex set $V(Q_n) = \{0,1\}^n$ and in which two vertices are adjacent if they differ in exactly one co-ordinate.

Example 4.3.1.



Practice 4.3.2

Show how you can make Q_n from two copies of Q_{n-1}.

A *Gray code of order n* is a path (a sequence of distinct vertices in which consecutive vertices are joined by an edge) in Q_n that visits each vertex exactly once. (This is also called a *Hamilton path* in Q_n, and is something we will look at for other graphs later.)

Practice 4.3.3

Find a Gray code of order 3.

Gray codes are nice because they give a listing of the subsets of $[n]$ in which consecutive subsets differ only in one element. But generally we do not define them with graphs. Or real definition of a *Gray code* of order n is a listing of all 2^n strings in $\{0,1\}^n$ such that consecutive strings differ in one co-ordinate.

Again, there is an easy algorithm for generating an order n Gray code from an order $n-1$ one.

i. Write the strings of the Gray code of order $n-1$, one per line, in a list, and append a 0 to the start of each.

ii. Below this, write them again, one per line, but going from the last one to the first, and append a 1 to the start of each.

Starting with the Gray code $0, 1$ of order 1, the gray code of order n we get by repeating the above recursive construction is called the *reflected Gray code* of order n.

Practice 4.3.4

Generate the reflected Gray code of order 3 this way. Convert each string to an integer, and write the Gray code as a permutation of $[8]$.

Practice 4.3.5

In the Gray code of order 8 constructed in this way, what set follows $\{1, 2, 5, 6, 8\}$?

Lets formalise that.

Theorem 4.3.2. *Let $(v_n, v_{n-1}, \ldots, v_1)$ be a string in $\{0,1\}^n$. To get the next element in the reflected Gray code of order n:*

i. if the sum of the digits is even then change v_1, otherwise

ii. change v_{i+1} where v_i is the rightmost (smallest index) 1.

Before we start the proof, lets make some easy observations and convenient notation. Let $G_n(i)$ denote the i^{th} string in the reflected Gray code of order n, so the code is $G_n(1), G_n(2), \ldots, G_n(2^n)$. Call $G_n(i)$ even or odd if the sum of its digits is even or odd. We will use the following easy observations:

Practice 4.3.6

Show that

- $G_n(i)$ is even if and only if i is odd.
- $G_n(2^n) = (1, 0, 0, \ldots, 0)$,
- $G_n(2^{n-1} - 1) = (0, 1, 0, 0, \ldots, 0)$,
- $G_n(2^{n-1}) = (1, 1, 0, 0, \ldots, 0)$

.

For a string v of length $n-1$ and a bit $b \in \{0,1\}$, let $b|v$ be the string of length n we get by appending the bit b to the right of v. So

$$G_n(i) = \begin{cases} 0|G_{n-1}(i) & \text{if } i \leq 2^{n-1} \\ 1|G_{n-1}(2^n - i + 1) & \text{if } i > 2^{n-1} \end{cases}.$$

With this notation, we are ready to prove the theorem.

Proof. The proof is by induction, and is clear for the case $n = 1$. Assume that it is true for the reflected Gray code of order $n-1$ and that $G_n(i) = (v_n, v_{n-1}, \ldots, v_1)$. There are three cases: $i \leq 2^{n-1} - 1, i = 2^{n-1}$, and $i > 2^{n-1}$.

In the first case we have $G_n(i)$ and $G_n(i+1)$ both start with 0, so have the same parity as $G_{n-1}(i)$ and $G_{n-1}(i+1)$ respectively, and so the result is trivial by inducion (as appending a 0 does not change what the rightmost 1 is).

In the second case, $i = 2^{n-1}$ we have that $G_n(i) = (0, 1, 0, 0, \ldots, 0)$ and $G_n(i+1) = (1, 1, 0, 0, \ldots, 0)$ and so as i is even, so $G_n(i)$ is odd, this is as it should be.

So we may assume we are in the third case with $2^{n-1} < i < 2^n$. (If $i = 2^n$ there is nothing to show.) Thus $G_n(i) = 1|G_{n-1}(2^n - i + 1)$ and $G_n(i+1) = 1|G_{n-1}(2^n - i)$, and so to get from $G_n(i)$ to $G_n(i+1)$ we go

$$G_n(i) \overset{\text{remove initial 1}}{\longrightarrow} G_{n-1}(2^n - i + 1) \overset{\text{go UP}}{\longrightarrow} G_{n-1}(2^n - i) \overset{\text{replace 1}}{\longrightarrow} G_n(i+1).$$

If $G_n(i)$ is even, then $G_{n-1}(2^n - i + 1)$ is odd, and so $G_{n-1}(2^n - i)$ is even and so $G_{n-1}(2^n - 1)$ and $G_{n-1}(2^n - i + 1)$ differ in v_1, thus $G_n(i)$ and $G_n(i+1)$ do, as needed. If $G_n(i)$ is odd, the so is $G_{n-1}(2^n - i)$, so we get from it to $G_{n-1}(2^n - i + 1)$ by switching the place to the left of the rightmost 1. The rightmost 1 does not change by this, and so is also the rightmost 1 of $G_{n-1}(2^n - i + 1)$ and so of $G_n(i)$, and so we get from $G_n(i) = 1|G_{n-1}(2^n - i)$ to $G_n(i+1) = 1|G_{n-1}(2^n - i + 1)$ by switching the place to the left of its rightmost 1, as required.

□

We skip Section 4.4 and 4.5 but will use some of the definitions from 4.5 later. I expect that you know many of them from high school or a set theory class. Definitions of such things as: orders, partial orders, relations, transitivity, reflexivity, symmetry, equivalence relations, partitions. If you don't please read them.

Problems from the Text

Sect 4.6: 6, 7, 8, 15, 20

Chapter 5

The Binomial Coefficient

In this chapter we look at a bunch more identites involving binomial coefficients.

5.1 Pascal's Triangle

You've probably drawn out Pascal's Triangle once or twice:

$$\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & & 1 & & & & & & & & & & \\
 & & & & & & & & 1 & & 1 & & & & & & & & \\
 & & & & & & & 1 & & 2 & & 1 & & & & & & & \\
 & & & & & & 1 & & 3 & & 3 & & 1 & & & & & & \\
 & & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & \\
 & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & \\
\end{array}$$

You start with the 1s, and otherwise, each entry is the sum of the two next entries diagonally above it.

Practice 5.1.1

Use Pascal's identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ to show that (counting from 0) the k^{th} entry in the n^{th} row is $\binom{n}{k}$.

So Pascal's triangle is often written like this:

$$\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & & \binom{0}{0} & & & & & & & & & & \\
 & & & & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & & \\
 & & & & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & & \\
 & & & & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & & \\
 & & & & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & & \\
 & & & & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & & & \\
\end{array}$$

This magical little triangle yields lots of cool identies. Here is a new proof of one that we have seen before.

Practice 5.1.2

Observing that the sum of the entries in a row is twice the sum of the entries in the previous row, show that

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

The number $\binom{n}{k}$ can be seen as the number of ways of getting from $\binom{n}{k}$ from $\binom{0}{0}$ by a combination of 'down left' and 'down right' steps. This answers the problem that you will see in the exercises of finding the number of shortest walks along a grid from one point to another.

5.2 The Binomial Theorem

With a combinatorial argument about the number of ways of choosing k different xs in the expansion of $(x+y)^n$, we proved the Binomial Theorem.

Theorem 5.2.1. *For a positive integer n the following holds:*

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

Let's prove it again, but this time by induction. (Combinatorial arguments are nicer for those who like pictures. But an arithmetic proof makes everybody feel safer.)

Proof. Our induction is on n. When $n = 1$ we have

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

as needed.

Assuming now that the identity holds for $(x+y)^{n-1}$ we have

$$\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} = (x+y)\sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-1-k}y^k \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-1-k}y^{k+1} \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{k=1}^{n}\binom{n-1}{k-1}x^{n-k}y^k \\
&= \binom{n-1}{0}x^n y^0 + \sum_{k=1}^{n-1}\left(\binom{n-1}{k} + \binom{n-1}{k-1}\right)x^{n-k}y^k + \binom{n-1}{n-1}x^0 y^n \\
&= \binom{n-1}{0}x^n y^0 + \sum_{k=1}^{n-1}\binom{n}{k}x^{n-k}y^k + \binom{n-1}{n-1}x^0 y^n
\end{aligned}$$

We are done by observing that the outside binomial coefficients are 1 so can be replaced with those in the desired identity. □

Taking $x = y = 1$ in this theorem again gives

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}. \tag{5.1}$$

Taking $x = 1$ and $y = -1$ gives

$$0 = \binom{n}{0} - \binom{n}{1} + \cdots \pm \binom{n}{n},$$

which yields that

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

Another useful identity is the following, which we can argue by double counting the number of ways to choose a k member team, with a captain, from n people:

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{5.2}$$

Practice 5.2.1

Using the identites (5.1) and (5.2) show that

$$n2^{n-1} = \sum_{i=1}^{n} i\binom{n}{i}.$$

You can also get this last identity with calculus: take the derivative of

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

with respect to x to get

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

and then put $x = 1$.

There are several more interesting identities in the text, but we skip them. We finish this section simply by giving a more general definition of the binomial co-efficeints. One of your homework problems will ask you something about them.

Definition 5.2.2. For any real number n and any integer k (not necessarily positive) let

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)\ldots(n-k+1)}{k!} & \text{if } k \geq 1 \\ 1 & \text{if } k = 0 \\ 0 & \text{if } k \leq -1 \end{cases}.$$

With this definition one can show that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \text{and} \quad k\binom{n}{k} = n\binom{n-1}{k-1}$$

still hold.

5.3 Unimodality of Binomial Coefficients

A sequence of numbers

$$s_1, s_2, \ldots, s_n$$

is *unimodal* if there is an index $t \in [n]$ such that

$$s_1 \leq s_2 \leq \cdots \leq s_t \geq s_{t+1} \geq \cdots \geq s_n,$$

or the same with the inequalities reversed. The number s_t is the *mode*.

Theorem 5.3.1. *For all $n \geq 1$, the sequence $s_0, \ldots, s_n$ where $s_i = \binom{n}{i}$ is unimodal with mode $\binom{n}{n/2}$ if n is even, and with modes $\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$ if n is odd.*

Proof. Consider the ratio

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

This is one if $k = (n+1)/2$. It is greater than one if $k < (n+1)/2$, and less than one if $k > (n+1)/2$. □

Sperner's Theorem

What is the biggest family $\mathcal{A} \subset 2^{[n]}$ of subsets of $[n]$ such that no subsets in the family is contained in another?

Note:
If you are unfamiliar with the definitions of partial orders or posets, they are given in more deali in Section 4.5 the text.

The set 2^S of subsets of a set S is a poset under inclusion: that is, the relation $\subseteq$ is reflexive, transitive and antisymmtric. (In fact, it is a lattice.) A *chain* in a poset is a totally ordered subset, and an *antichain* is a set of pairwise incomparible elements.

The question above was asking for the largest antichain in the poset $2^{[n]}$. Notice that the family of i-subsets of $[n]$ is an antichain in $2^{[n]}$. Taking $i = \lfloor n/2 \rfloor$, we get an antichian of size $\binom{n}{\lfloor n/2 \rfloor}$. Is this the largest?

We will answer this in a second, but first lets look at some easier questions.

Practice 5.3.1

How long is the longest chain in $2^{[n]}$? How many longest chains are there in $2^{[n]}$? How many longest chains contain a particular k-set?

It follows from your answers here that any subset in $2^{[n]}$ is contained in at least $\lfloor n/2 \rfloor! \lceil n/2 \rceil!$ longest chains. With this we can prove the following.

Theorem 5.3.2. *The largest antichain in* $2^{[n]}$ *contains* $\binom{n}{\lfloor n/2 \rfloor}$ *elements.*

Proof. Let $\mathcal{A}$ be an antichain in $2^{[n]}$. As no two elements in $\mathcal{A}$ can be in the same longest chain in $2^{[n]}$, and each element is in at least $\lfloor n/2 \rfloor! \lceil n/2 \rceil!$ we have that

$$|\mathcal{A}| \leq \frac{n!}{\lfloor n/2 \rfloor! \lceil n/2 \rceil!} = \binom{n}{\lfloor n/2 \rfloor!}.$$

□

5.4 Multinomial Coefficients

As the binomial coefficients $\binom{n}{k}$ are the coefficients in the expansion of the binomial

$$(x + y)^n$$

we can talk also of the coefficients in the expansion of the multinomial

$$(x_1 + x_2 + \cdots + x_t)^n.$$

Observe that ever monomial in the expansion of this polynomial is of the form

$$x_1^{n_1} x_2^{n_2} \ldots x_t^{n_t}$$

where $n = n_1 + \cdots + n_t$.

Practice 5.4.1

For a given decomposition $n = n_1 + \cdots + n_t$ of n into positive integers n_i how many times does the monomial $x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$ appear in the expansion of $(x_1 + x_2 + \cdots + x_t)^n$?

Defining the *multinomial coefficient*

$$\binom{n}{n_1\, n_2\, \dots\, n_t} = \frac{n!}{n_1! n_2! \dots n_t!}$$

for non-negative integers $n_1, \dots, n_t$ whose sum is n we get, this yields the following theorem.

So observe that $\binom{n}{k}$ can be written as $\binom{n}{k\,(n-k)}$.

Theorem 5.4.1. *Let n be a positive integer. For all $x_1, \dots, x_t$ we have*

$$(x_1 + x_2 + \cdots + x_t)^n = \sum \binom{n}{n_1\, n_2\, \dots\, n_t} x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$$

where the sum runs over all decompositions $n = n_1 + \cdots + n_t$ of n into non-negative integers n_i.

Practice 5.4.2

Give a combinatorial proof that Pascal's formula holds for multinomial coefficients:

$$\binom{n}{n_1\, n_2\, \dots\, n_t} = \binom{n-1}{n_1 - 1\, n_2\, \dots\, n_t} + \binom{n-1}{n_1\, n_2 - 1\, \dots\, n_t} + \cdots + \binom{n-1}{n_1\, n_2\, \dots\, n_t - 1}.$$

Practice 5.4.3

What is the multinomial analogue of Pascal's Triangle?

Practice 5.4.4

What is the coefficient of $x_1 x_2^2 x_4^6$ in the expansion of $(x_1 + x_2 + \cdots + x_5)^9$?

Problems from the Text

Sect 5.7: 6, 7, 8, 14, 23

Chapter 6

The Inclusion Exclusion Principle and its Applications

In this chapter we give the promised extension of the subtraction principle for counting.

6.1 The Inclusion Exclusion Principle

Let's introduce the inclusion exclusion principle with a simple example.

Practice 6.1.1

What is the number of permutation in [10]! in which 1 isn't in the first position? What is the number in which 1 isn't in the first position **and** 2 isn't in the second position?

Solution

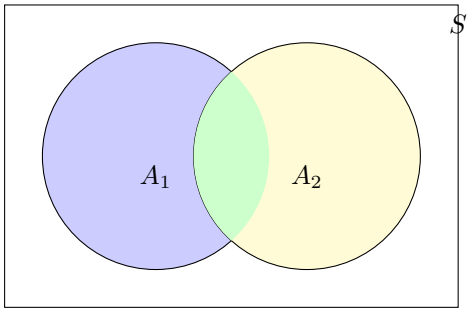
There are 10! permutations of [10]. There are 9! in which one is in the first position. So by the substitution principe there are $10! - 9!$ permuation in which 1 isn't in the first position. There are 9! in which 2 is in the second position. There are 8! in which neither 1 is in the first position and 2 in the second. So

$$10! - 9! - 9! + 8!$$

in which 1 isn't in the first positio **and** 2 isn't in the second position?

Easy, eh? I'm going to write this solution out again with some notation that we are going to use systematically for such problems.

Let S be the set of permutations of [10]. Let $A_1 \subset S$ be those permutatons such that '1 is in the first spot', and let A_2 be thoses such that '2 is in the second spot'.



The number we want to count is the white part of the diagram: $|S - A_1 - A_2|$. If we try to count $|S| - |A_1| - |A_2|$ there there are some green permutations in $A_1 \cap A_2$ that we have subtracted twice. We have to put those back in and count

$$|S - A_1 - A_2| = |S| - |A_1| - |A_2| + |A_1 \cap A_2| = 10! - 9! - 9! + 8!.$$

Try taking it a step further.

Practice 6.1.2

How many numbers from 1 to 120 are relatively prime to 30.

The principle of inclusion exclusion (PIE) is then.

Theorem 6.1.1. *Let S be a set, and for $i = 1, \ldots, m$ let A_i be the subset of elements satisfying property P_i. For a subset $I \subset [n]$ let a_I be $|\bigcap_{i \in I} A_i|$, (and let $a_0 = |S|$.) The number of elements satisfying none of the properties P_i is*

$$|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| = \sum_{i=0}^{m} (-1)^i \sum_{I \in \binom{[m]}{i}} a_I.$$

Proof. Elements in S having none of the properties P_i are counted in a_0 and contribute nothing else to the sum, so it is enough to check that for elements having some of the properties P_i, the element contributes 0 to the sum. Let e be an element and let $J = \{j \mid e \text{ satisfies property } P_i\}$. Then e contributes $(-1)^{|I|}$ to the sum for each $I \subset J$. But where $|J| = j$, there are $\binom{j}{1}$ subsets of J of size I, and $\binom{j}{2}$ of size 2, etc. So e contributes

$$\binom{j}{0} - \binom{j}{1} + \binom{j}{2} - \cdots \pm \binom{j}{j} = 0.$$

□

Practice 6.1.3

(From text) How many permuations of the set $\{M, A, T, H, I, S, F, U, N\}$ contain none of the words MATH or IS or FUN occuring consucutively in that order.

The following corollary is the version we would use to solve the Practice problem about number of integers in [120] being prime to 30.

Corollary 6.1.2. *The number of objects of S with at least one of the properties P_i is*

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{i=1}^{m} (-1)^{i+1} \sum_{I \in \binom{[m]}{i}} a_I.$$

6.2 Combinations with Repetition

It was easy to find the number of r-combinations of a multiset with infinite repetitions:

$$\{\infty \cdot 1, \infty \cdot 2, \infty \cdot 3\}.$$

We didn't find it if the number of repetitions was finite though. This was harder. The infinite repetition case we could solved as follows.

Example 6.2.1. The number of solutions of

$$x_1 + x_2 + x_3 = r$$

is $\binom{r+2}{2}$. We got this by arranging 2 separators and r items.

We were able to deal with variations such as the requirement that $x_1 \geq 3$. But we couldn't deal with the requirement that $x_1 \leq 3$, which we would need to find the number of r combinations of

$$\{3 \cdot 1, \infty \cdot 2, \infty \cdot 3\}.$$

We do this now using PIE

Practice 6.2.1

Find the number of solutions of

$$x_1 + x_2 + x_3 = 14$$

such that $x_1 \leq 5, x_2 \leq 6$, and $x_3 \leq 5$.

6.3 Derangements

A *derangement* of $[n]$ is a perm $(a_1, a_2, \ldots, a_n)$ of $[n]$ such that $a_i \neq i$ for all i.

Example 6.3.1. There are no derangements of [1]. The only derangement of [2] is 21. There are two derangements of [3]: 231 and 312.

Let D_i denote the number of derangements of $[i]$, so we have $D_1 = 0, D_2 = 1$, and $D_3 = 2$.

Theorem 6.3.2. *For $n \geq 1$*

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

Proof. See text. □

Note

Recall the Maclaurin expanison

$$e^x = 1 + x/1! + x^2/2! + x^3/3! + \ldots.$$

Putting $x = -1$ we get

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right) \approx n!/e.$$

The probability that a random permutation is a derangement is approximately $1/e$.
One can show that for i not too big the sum $1/i! + 1/(i+1)! + \ldots$ converges to something less than $1/2$ and so this approximation is really good: D_i is the closest integer to $n!/e$.

That was fun. There is another way to get an exact formula for the number D_n. We will see it in the next chapter when we see how to solve recurrence relations. To motivate recurrence relations for us we now make some relevant observations about the values D_n.

How might we find the exact value of D_n! We have a long inclusion-exclusion formula, but one might also observe that we can get D_n from D_{n-1} and D_{n-2}:

Consider the derangements of $(a_1 \ldots, a_n)$ of n with $a_n = n - 1$. Either

- $a_{n-1} = n$ and $(a_1, \ldots, a_{n-2})$ is a derangement of $[n-2]$, or
- $a_{n-1} \neq n$, and replacing n is $(a_1 \ldots, a_{n-1})$ with $n-1$ we get a derangment of $[n-1]$.

So there are $D_{n-1} + D_{n-2}$ derangements with $a_n = n - 1$. We can to the same counting for the derangements with $a_n = i$ for any of the $n-1$ values of $i \in [n-1]$. So there are $(n-1)(D_{n-1}+D_{n-2})$ derangements of $[n]$.

We can then compute from $D_1 = 0, D_2 = 1$, and $D_3 = 2$ that

$$D_4 = 3(D_3 + D_2) = 3(1+2) = 9 \quad \text{and} \quad D_5 = 4(D_4 + D_3) = 4(9+2) = 44.$$

This is a recurrence relation for the numbers D_n. It is nice to know these even if we can compute the numbers in a closed form, because then we can recognise them in combinatorial problems.

The above relation has another common form.

Practice 6.3.1

Using the above relation for D_i show that

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

Problems from the Text

Sect 6.7: 3, 5, 8, 9, 13, 15, 19, 20, 21

Chapter 7

Recurrence Relations and Generating Functions

7.1 Recurrence Relations

Given a sequence

$$h_1, h_2, h_3, \ldots,$$

of numbers, a recurrence relation is a formula that allows us to compute later terms in the sequence from earlier terms in the sequence. In the last Chapter we saw a recurrence relation (in fact two of them) for the sequence of derangement numbers D_1, D_2, D_3: we said that $D_1 = 0, D_2 = 1$ and that for $i \geq 3$, $D_i(i-1)(D_{i-1} + D_{i-1})$. This is enough to define the whole sequence, recursively.

Certainly $h_1 = 2$ and $h_i = h_{i-1}^2 - 1$ for $I \geq 2$ is a recurrence relation defining a sequence

$$2, 3, 8, 63, \ldots,$$

but we won't consider such relations. The recurrence relations we will consider going to be 'linear', which means in that our formula for h_i is linear in the earier terms. Such powers as h_{i-1}^2 are not allowed.

Here is a simple example of a linear recurrence relation.

Example 7.1.1. Let $h_0, h_1, h_2, h_3, \ldots,$ be defined by $h_0 = 1$ and $h_n = h_{n-1} + 3$ for $n \geq 1$.

The first thing we are going to do with a recurrence relation is to solve it. It is easy to see by writing out some terms or the sequence:

$$1, 4, 7, 10, 13, \ldots,$$

that it can also be described by the closed formula $h_n = 1 + 3n$. A *closed* formula is one that we can compute quickly without first computing earlier terms. It depends only on the index i of h_i. *Solving* a recurrence relation is finding a closed formula for it. In fact you probably didn't even

have to write out a couple terms to solve this recurrence relation. The closed formula was probably obvious. It isn't always.

Here is another example of a linear recurrence relation– one that you are probably quite familiar with.

Example 7.1.2. The *Fibonacci numbers* $f_0, f_1, \ldots$, are defined by

$$f_0 = 0, f_1 = 1 \text{ and } f_n = f_{n-1} + f_{n-2} \text{ for } n \geq 2.$$

You know this sequence well, it often is written like this:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Possibly you have solved the fibonacci recurrence before, maybe in a linear algebra class. We will here too, but before we do, lets look at some identities that arise easily from the description of this sequence as a recurrence relation. Easy identities are one of the benefits of recurrence relations.

Practice

Show that the partial sum $s_n = f_0 + f_1 + \cdots + f_n$ is equal to $f_{n+2} - 1$.

Practice

Show that f_n is even if and only if n is divisible by 3.

Practice

Find the number h_n of perfect covers of a $n \times 2$-chessboard with dominoes.

Do you see the Fibonacci numbers in Pascal's Triangle?

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\end{array}$$

I'm having trouble drawing the lines in these notes, but if you sum up along the right lines you will find them. The following problem, a theorem from the book, explains what lines. (Finding the lines will help you see the proof.)

Practice

Show that for all $n =\geq 1$ the n^{th} fibonacci number is

$$f_n = \binom{n-1}{0} + \binom{n-2}{1} + \cdots + \binom{n-t}{t-1}$$

where $t = \lfloor \frac{n+1}{2} \rfloor$.

In Section 7.4 we will solve the the fibonacci recurrence relation, in fact, we will solve it twice. In one of our solutions we will use a useful tool known as a generating function. We introduce this now.

7.2 Generating Functions

Given a sequence

$$h_1, h_2, h_3, \ldots,$$

the *generating function* $g(x)$ of the sequence is the formal power series

$$g(x) = h_0 + h_1 x + h_2 x^2 + \ldots.$$

When we call it a 'formal' power series, it emphasises the fact that we will not worry about such things as convergence. It is an algebraic construction.

A generating function allows compact representation of sequences, and useful manipulations. Finding a generating function for a sequence will not always make computing a term of the sequnce easier, but sometimes it will.

Example 7.2.1. The generating function of the sequence $1, 1, 1, \ldots$, is the geometric sequence

$$g(x) = 1 + x + x^2 + x^3 + \ldots$$

which by a well known identity is $g(x) = \frac{1}{1-x}$.

Practice

Prove this identity and the related identity

$$1 + x + x^2 + x^3 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}.$$

What is the generating function of a sequence of six ones: $(1, 1, 1, 1, 1, 1)$?

Generating functions need not be infintie power series. They can be finite too.

Practice

The function $(1+x)^m$ is the generating function for what sequence?

We said that computing a co-efficient of a generating function will not always be easy. The following is an example of one that we can compute with a combinatorial arguement. What is the co-efficient of x^n in $\frac{1}{1-x}^k$?

We have to count the ways to choose a monomial from each of the k factors $\frac{1}{1-x} = (1 + x + x^2 + x^3 + \dots)$ so that the sums of their powers is n. We've seen this before. It is the number of non-negative integers solutions to

$$x_1 + x_2 + \cdots + x_k = n,$$

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

Using similar combinatorical arguments, one can find the generating function of a sequence, though computing the co-efficients may not be easy. You have i dollars to use at a fruit stand. Kiwi are 2 dollars each, pinepples are 3, and mangos are 5. Find the generating function $g(x) = \sum h_i x^i$ whose co-efficient h_i is the number of ways you can spend your i dollars on fruit?

Practice

Find the generating function $g(x) = \sum h_i x^i$ where h_i is the number of non-negative integers solutions to the equation

$$3x_1 + 4x_2 + 2x_3 + 5x_4 = i.$$

Practice

Find the generating function $g(x) = \sum h_i x^i$ where h_i is the number of non-negative integers solutions to the equation

$$x_1 + x_2 + x_3 = i$$

such that $0 \leq x_1 \leq 4$, $x_2 = 1 + 5c$ for some integer c, and $x_3 = 0$ or 1.

7.3 Exponential Generating Functions

Sometimes it is useful to use the exponential generating function of a sequence $h_1, h_2, h_3, \dots$:

$$g^{(e)}(x) = h_0 + h_1 x + h_2 \frac{x^2}{2!} + h_3 \frac{x^3}{3!}.$$

Practice

Show that the i^{th} derivative $(g^{(e)})^{[i]}(x)$ of $g^{(e)}$ evaluated at $x = 0$ is h_i.

Practice

What is the exponential generating function of $1, 1, 1, \ldots$? Why is it called the exponential generating function?

Practice

What sequence has exponential generating function $g^{(e)}(x) = e^{ax}$?

In the same way that the generating function was useful in r-combination problems, the exponential generating function is useful in r-permutation problems.

Theorem 7.3.1. *Let h_r be the number of r-permutations of the multiset*

$$\{n_1 \cdot a_1, n_2 \cdot a_2, \ldots, n_k \cdot a_k\}.$$

The exponential generating function $g^{(e)}$ of $h_0, h_1, h_2, \ldots,$ is

$$g^{(e)} = f_{n_1}(x) f_{n_2}(x) \ldots f_{n_k}(x)$$

where $f_{n_i}(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n_i}}{n_i!}$ for all i.

Proof. The co-efficient of x^n is the sum

$$\sum \frac{1}{m_1! m_2! \ldots m_k!}$$

over all partitions $n = m_1 + \cdots + m_k$ with $0 \leq m_i \leq n_i$. So

$$h_n = \sum \frac{n!}{m_1! m_2! \ldots m_k!}.$$

This is the number of n-permutations of the set. □

This reasoning can be applied to more restrictive r-permutation problems.

Example 7.3.2. Let h_n be the number of n-permuations of the multiset

$$\{\infty \cdot a_1, \infty \cdot a_2, \infty \cdot a_3\}$$

such that a_2 occurs an odd number of times and a_3 occurs at least once.

The exponential generating function $g^{(e)}(x)$ for $h_0, h_1, h_2, \ldots,$ is

$$\begin{aligned} g^{(e)}(x) &= (1 + x + \frac{x^2}{2!} + \ldots) \\ &\cdot \quad (x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots) \\ &\cdot \quad (x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots). \end{aligned}$$

Using that $e^x = 1 + x + \frac{x^2}{2!} + \ldots$ we get that

- $e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$
- $e^x + e^{-x} = 2(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \dots$
- $e^x - e^{-x} = 2(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \dots.$

Thus we can express the above more compactly as

$$\begin{aligned} g^{(e)}(x) &= e^x \cdot (\frac{e^x - e^{-x}}{2}) \cdot (e^x - 1) \\ &= \frac{1}{2}(e^{2x} - 1)(e^x - 1) \\ &= \frac{1}{2}(e^{3x} - e^{2x} - e^x + 1) \end{aligned}$$

Again using $e^x = 1 + x + \frac{x^2}{2!} + \dots$ we get that

- $e^{2x} = 1 + 2x + 2^2\frac{x^2}{2!} + \dots$
- $e^{3x} = 1 + 3x + 3^2\frac{x^2}{2!} + \dots.$

So this is

$$g^{(e)}(x) = \frac{1}{2}\left(\sum \frac{x^i}{i!}(3^i - 2^i - 1)\right) + 1/2.$$

Thus $h_0 = 1/2 - 1/2 = 0$ and for $n \geq 1$ we have

$$h_n = \frac{1}{2}(3^n - 2^n - 1).$$

There are many similar examples in the text. You should look at a couple. Indeed, the following problems are (similar to) worked examples in the text. They can all be viewed as counting n-permutations of a multiset with infinite mutliplicities, and various restrictions. You should be able to find the exponential generating function and then put it in a form in which you can read off the coefficients.

Practice

Determine the number of ways to color the squares of a $1 \times n$ chessboard with the colours blue, green, and red, if the number of red squares will be even.

Practice

Let h_n be the number of ways of stringing together a string of n beads of colours red, yellow, blue and white, so that there are an even number of red and blue beads. Find the exponential generating function for $h_0, h_1, \dots,$

7.4 Linear Homogeneous Recurrence Relations

A *recurrence relation* for a sequence $h_0, h_1, \ldots$, is a function that for large enough n defines h_n in terms of n and h_i for $i < n$. The ones we consider are *linear homogeneous recurrence relations with constant co-efficients*: recurrence relations of the form

$$h_n = a_1 h_{n-1} + a_2 h_{n-2} + \cdots + a_k h_{n-k}.$$

The term *linear* because the function is linear in all previous terms h_i that occur. It is *homogeneous* because every summand has the same degree 1: no summands such as $h_{n-1}h_{n-2}$ or terms without any h_i. It has *constant coefficient* because the a_i do not depend on n. Recall that the number D_n of derangements of $[n]$ was $D_n = (n-1)(D_{n-1} + D_{n-2})$. This recurrence relation doesn't have constant co-efficeints. It's too hard for us. We deal with guys like the Fibonacci relation $f_n = f_{n-1} + f_{n-2}$. In fact, we will see two proofs that

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

(In fact we see two derivations. A proof is actually easier.)

If we can get any formula $f(n)$ such that $f(0) = 0, f(1) = 1$ and $f(n) = f(n-2) + f(n-1)$ for all $n \geq 2$ then this is a solution of the recurrence: then $f(n) = f_n$. We 'guess' that there is a formula of the form $f(n) = q^n$, and derive what it must look like.

Such a formula must satisfy:

$$\begin{aligned} & q^n = q^{n-1} + q^{n-2} \\ \rightarrow \quad & q^{n-2}(q^2 - q - 1) = 0 \\ \rightarrow \quad & q = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2} \end{aligned}$$

So $f(n) = \left(\frac{1+\sqrt{5}}{2}\right)^n$ and $f(n) = \left(\frac{1-\sqrt{5}}{2}\right)^n$ both satisfy our recurrence. Oh, but neither of them have $f(0) = 0$. No problem, as the relation is linear, any linear combination

$$f(n) = \left(\frac{1+\sqrt{5}}{2}\right)^n \quad \text{and} \quad f(n) = \left(\frac{1-\sqrt{5}}{2}\right)^n$$

$$f(0) \neq 0 \quad \text{and} \quad f(1) \neq 1.$$

$$f(n) = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

also satisfies the recurrence. Choosing c_1 and c_2 properly we get our solution:

$$0 = f_0 = c_1\left(\frac{1+\sqrt{5}}{2}\right)^0 + c_2\left(\frac{1-\sqrt{5}}{2}\right)^0 = c_1 + c_2$$

and

$$\begin{aligned} 1 = f_1 &= c_1\left(\frac{1+\sqrt{5}}{2}\right)^1 + c_2\left(\frac{1-\sqrt{5}}{2}\right)^1 \\ &= c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_1\left(\frac{1-\sqrt{5}}{2}\right) \\ &= \frac{1}{2}(\sqrt{5}(c_1+c_1)) = c_1\sqrt{5} \end{aligned}$$

Thus $c_1 = \frac{1}{\sqrt{5}}$ and $c_2 = -\frac{1}{\sqrt{5}}$, giving the needed

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

That wasn't terrible, but a bit mucky. We don't really to do it for more complicated recurrences to often. And what about that mysterious 'guess' that $f(n) = q^n$ should solve our relation? That will always work, and the same calculations will usually work.

Theorem 7.4.1. *Let q be a non-zero number. Then $h_n = q^n$ is a solution to the recurrence*

$$h_n = a_1 h_{n-1} + a_2 h_{n-2} + \cdots + a_k h_{n-k}$$

where $a_k \neq 0$ and $n \geq k$, if and only if q is a root of

$$x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - = 0. \tag{7.1}$$

If the polynomial has distinct roots $q_1, \ldots, q_k$, then

$$h_n = c_1 q_1^n + c_2 q_2^n + \cdots + c_k q_k^n$$

is the general solution to the recurrence relation: for any choice of values of $h_0, \ldots, h_k$ there are constants $c_1, \ldots, c_k$ that solve the relation for these initial values.

Note

We will not prove this, but the first statement follows by computations just like those we did for the Fibonacci recurrence. By linearlty, $h_n = c_1 q_1^n + c_2 q_2^n + \cdots + c_k q_k^n$ is also a solution to the recurrence by linearly whether or not the roots are distinct. However, if they are not distinct, there are other solutions. If they are distinct, then we have k linearly independent equations (this requires a proof) in k unknowns, so there is a solution.

We now look at solving the same relation again, using generating functions.

First, we find a generating function $g(x)$ for the Fibonacci recurrence $f_n = f_{n-1} + f_{n-2}$, (without initial values):

$$\begin{array}{lcccccc} g(x) & = & f_0 & +xf_1 & +x^2f_2 & +x^3 & +\dots \\ -xg(x) & = & & -xf_0 & -x^2f_1 & -x^3f_2 & -\dots \\ -x^2g(x) & = & & & -x^2f_0 & -x^3f_1 & -\dots \end{array}$$

Summing both sides we get $g(x)(1-x-x^2) = f_0 + x(f_1 - f_0) = x$, which we rearrange to get $g(x) = \frac{x}{1-x-x^2}$. Finding roots

$$d_1 = \frac{-1+\sqrt{5}}{2} = \frac{2}{1+\sqrt{5}}$$
$$d_2 = \frac{1+\sqrt{5}}{-2} = \frac{2}{1-\sqrt{5}},$$

Note

This *characteristic polynomial* $(1-x-x^2)$ is independent of the initial values f_0 and f_1. The numerator x depends on the initial values.

we factor $(1-x-x^2) = -(x-d_1)(x-d_2)$. We can then expand $g(x)$ into partial fractions.

Setting

$$g(x) = \frac{-x}{(x-d_1)(x-d_2)} = \frac{c_1}{(x-d_1)} + \frac{c_2}{(x-d_2)},$$

we equate coefficients and get the equations

$$-1 = c_1 + c_2 \qquad \text{and} \qquad 0 = c_1d_2 + c_2d_1.$$

Solving these yields

$$c_1 = \frac{d_1}{d_2-d_1} = \frac{-1}{\sqrt{5}}d_1 \qquad \text{and} \qquad c_2 = \frac{d_2}{d_1-d_2} = \frac{1}{\sqrt{5}}d_2$$

and so

$$\begin{aligned} g(x) &= \frac{1}{\sqrt{5}}\left(\frac{d_1}{d_1-x} - \frac{d_2}{d_2-x}\right) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-x/d_1} - \frac{1}{1-x/d_2}\right) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1}{1-x\frac{1+\sqrt{5}}{2}} - \frac{1}{1-x\frac{1-\sqrt{5}}{2}}\right) \\ &= \frac{1}{\sqrt{5}}\left((1+x\left(\frac{1+\sqrt{5}}{2}\right) + x^2\left(\frac{1+\sqrt{5}}{2}\right)^2 + \dots) \right.\\ &\qquad \left. -(1+x\left(\frac{1-\sqrt{5}}{2}\right) + x^2\left(\frac{1-\sqrt{5}}{2}\right)^2 + \dots)\right) \end{aligned}$$

Reading off the coefficient of x^n we get

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

This was a bit messy because of the ugly roots of the characteristic polynomial. Try it on your own with this cleaner example from Page 235 of the text.

Practice

Solve the recurrence relation

$$h_n = 5h_{n-1} - 6h_{n-2} \qquad (n \geq 2)$$

with initial conditions $h_0 = 1$ and $h_1 = -2$.

Problems from the Text

Sect 7.7: 3(c), 11(a), 15, 18, 25, 33,40

Chapter 8

Special Counting Sequences

In this chapter we will introduce several sequences that are nice for counting various things. Like the fibonacci numbers and the binomial co-efficients, there are all sorts of identities about and relating these sequences. We will see only the tip of the iceberg.

8.1 The Catalan numbers

The n^{th} *Catalan number* C_n is the number of *n-bracketings* : ways to write n pairs of brackets so that each open bracket has a corresponding, uniquely paired, closed bracket to its right.

n	n-bracketings	C_n
0		1
1	( )	1
2	(( )), ()()	2
3	((( ))), (())(), (()()), ()((()), ()()()	5

We will prove the following.

Theorem 8.1.1. $C_n = \frac{1}{n+1}\binom{2n}{n}$.

Before we prove this theorem though, let's look at a more convenient representation of C_n. Replacing each '(' with a $+1$ and each ')' with a -1 we get a 1-to-1 correspondence between the n-bracketings and the $2n$-term sequences $(a_1, \ldots, a_{2n})$ in $\{-1, 1\}^{2n}$, every partial sum $S_\alpha := \sum_{i=1}^{\alpha} a_\alpha$ of which is non-negative. Rather than counting n-bracketings, we count such sequences.

Proof. Call a sequence $(a_1, \ldots, a_{2n})$ in $\{-1, 1\}^{2n}$ is a 0-sequence if it sums to 0. It is *good* if each partial sum S_α is non-negative. There are $\binom{2n}{n}$ 0-sequences in $\{-1, 1\}^{2n}$. We count those that are not good, or *bad*. And those that are bad, are really bad– like my youngest daughter Lisa. She says she likes jokes, but jokes shouldn't be so hurtful.

Consider a bad sequence, $a = (a_1, \ldots, a_{2n})$. Let k be the minimum integer such that $S_k < 0$.

Then we have $a_k = -1$ and $S_{k-1} = 0$. Clearly k is odd, the sequence

$$-a_1, -a_2, \ldots, -a_{k-1}, -a_k, a_{k+1}, \ldots, a_{2n}$$

sums to 2, and the k^{th} partial sum of this sequence is the first that is positive.

On the other hand, consider a sequence $a = (a_1, \ldots, a_{2n})$ that sums to 2, and let k be the least integer such that $S_k > 0$. Then

$$-a_1, -a_2, \ldots, -a_{k-1}, -a_k, a_{k+1}, \ldots, a_{2n}$$

is bad, and the k^{th} partial sum is its first negative partial sum. So we have a 1-to-1 correspondence between bad sequences and sequences summing to 2. But there are clearly $\binom{(2n)!}{(n+1)!(n-1)!}$ of these, so this is how many bad seqences there are.

Thus

$$\begin{aligned} C_n &= \binom{2n}{n} - \frac{2n!}{(n+1)!(n-1)!} = \frac{2n!}{n!n!} - \frac{2n!}{(n+1)!(n-1)!} \\ &= \frac{2n!}{n!(n-1)!}\left(\frac{1}{n} - \frac{1}{n+1}\right) = \frac{2n!}{n!(n-1)!}\left(\frac{1}{n(n+1)}\right) \\ &= \binom{2n}{n}\frac{1}{n+1} \end{aligned}$$

as needed. □

From this formula for C_n we see that

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

So we get the recurrence $C_n = \frac{4n-2}{n+1}C_{n-1}$ with initial condition $c_0 = 1$.

Note

We skipped it, but in Section 7.6, it is shown, using generating functions, that the number of planar triangulations of a plane cycle on $n+2$ vertices is C_n. There is a cool combinatorial proof of this in Section 8.1 of the text.

Practice

Show that C_n counts the number of walks from the origin to (n, n) on an $n \times n$ grid that never goes below the diagonal line from $(0, 0)$ to (n, n).

The *pseudo Catalan numbers* C_n^* are defined by $C_1^* = 1$ and

$$C_n^* = n!C_{n-1} \text{ for } n \geq 2.$$

This yields a recursive formula:

$$\begin{aligned} C_n^* &= n!C_{n-1} = n!\frac{4n-6}{n}C_{n-2} = (n-1)!C_{n-2}4n-6 \\ &= (4n-6)C_{n-1}^*. \end{aligned}$$

These numbers count a structure related to bracketings that arises in algebra. A binary operation need not be associative, so for example, for some operation $\times$ we might have that $a \times (b \times c) \neq (a \times b) \times c$. In this case an expression such as

$$a \times b \times c$$

is not well defined– the results could be different depending on whether we compute it as

$$(a \times b) \times c \text{ or } a \times (b \times c).$$

Further, the operation need not be abelian, so

$$(a \times b) \times c \text{ and } (b \times a) \times c,$$

might be different.

Practice

Show by induction that $C_n^* = (4n-6)C_{n-1}^*$ counts the number of *multiplication schemes* for applying a non-associative, non-abelian operation $\times$ to n numbers?

8.2 Difference Sequences

In this Section we see the Catalan numbers and the Bell numbers.

Given a sequence $h_0, h_1, h_2, \ldots$, we make a difference table like you did in elementary school:

Example 8.2.1. The sequence $h_n = n^3$, which begins, $0, 1, 8, 27, 64, 125$ has difference table beginning

0		1		8		27		64		125
	1		7		19		37		61	
		6		12		18		24		
			6		6		6			
				0		0				
					0					

We denote the entries in the i^{th} row as $\Delta^i h_0, \Delta^i h_1, \ldots,$. They make up the i^{th} *degree difference sequence*. We don't have columns, but diagonals. The first entry of each row make up the 0^{th} *diagonal*.

Practice

In the above example, what are $\Delta^0 h_4$, $\Delta^1 h_3$, the 2^{nd} degree difference sequence $\Delta^2 n^3$ and the 1^{st} diagonal?

More precisely, let

i. $\Delta^1 h_j = h_{j+1} - h_j$, and

ii. $\Delta^i h_j = \Delta^1(\Delta^{i-1} h_j) = \Delta^{i-1} h_{j+1} - \Delta^{i-1} h_j$.

The following is clear:

Practice

$\Delta^i h_j = \Delta^{i-1}(\Delta^1 h_j)$.

Let's now look at a couple of easy properties of difference tables/sequences.

Practice

Where k_n and h_n are sequences, show for all i and j that

$$\Delta^i(a \cdot k_j + b \cdot h_j) = a\Delta^i k_j + b\Delta^i h_j.$$

Practice

Show that if $h_n = n^d$ then $\Delta^{d+1} h_i = 0$ for all i. Conclude that the same holds if $h_n = f(n)$ for any polynomial h of degree at most d.

Clearly the initial sequence $h = (h_1, h_2, \dots)$ determines the whole table, but it is not too hard to see that the 0^{th} diagonal does too. Indeed the i^{th} entry of the $(j+1)^{th}$ diagonal is the sum of the I^{th} and $(i+1)^{st}$ entries fo the j^{th} diagonal.

Practice

Find the difference table whose 0^{th} diagonal is $(0, 0, 0, 1, 0, 0, 0, \dots)$.

Use this practice exercise to show the following:

Theorem 8.2.2. *If the sequence $h_0, h_1, \dots,$ has 0^{th} diagonal $c_0, c_1, \dots, c_k, 0, 0, 0 \dots,$ then for all n*

$$h_n = c_0\binom{n}{0} + c_1\binom{n}{1} + c_2\binom{n}{2} + \cdots + c_k\binom{n}{k}$$

So what is this good for? Well, quite a bit, it turns out. Not only does it allow us to write polynomial function in the binomial basis, instead of the standard basis. But from this we get a

nice formula for partial sums of a polynomial sequence. You know a formula for $\sum_{i=1}^{n} i^2$ and for $\sum_{i=1}^{n} i^3$, but do you know one for $\sum_{i=1}^{n} i^4$? We will get one.

The first set is to write the function i^4 in a binomial basis.

Example 8.2.3. The difference table for $h_i = i^4$ is

$$\begin{array}{ccccccccccc}
0 & & 1 & & 16 & & 81 & & 256 & & \\
& 1 & & 15 & & 65 & & 175 & & 369 & \\
& & 14 & & 50 & & 110 & & 194 & & \\
& & & 36 & & 60 & & 84 & & 108 & \\
& & & & 24 & & 24 & & 24 & & \\
& & & & & 0 & & 0 & & 0 &
\end{array}$$

So we can write $i^4 = 1\binom{i}{1} + 14\binom{i}{2} + 36\binom{i}{3} + 24\binom{i}{4}$.

This seems an unneccesarily complicated way to write i^4, but recall that we wanted to sum this up from $i = 1$ to some n. So

$$\begin{aligned}
\sum_{i=0}^{n} i^4 &= 0\binom{1}{0} + 1\binom{1}{1} + 14\binom{1}{2} + 36\binom{1}{3} + 24\binom{1}{4} \\
&+ 0\binom{2}{0} + 1\binom{2}{1} + 14\binom{2}{2} + 36\binom{2}{3} + 24\binom{2}{4} \\
&\vdots \\
&+ 0\binom{n}{0} + 1\binom{n}{1} + 14\binom{n}{2} + 36\binom{n}{3} + 24\binom{n}{4}
\end{aligned}$$

Summing columnwise we get

$$\sum_{i=0}^{n} i^4 = 0\binom{n+1}{1} + 1\binom{n+1}{2} + 14\binom{n+1}{3} + 36\binom{n+1}{4} + 24\binom{n+1}{5}.$$

This is pretty cool. We only have to compute 4 summands, rather than n. And this works for any polynomial.

Theorem 8.2.4. *Let $f(n)$ be polynomial of degree d and $c_0, c_1, \ldots,$ be the 0^{th} diagonal of the difference table of $f(0), f(1), f(2), \ldots$. Then*

$$\sum_{i=0}^{n} f(n) = \sum_{i=0}^{d} c_i \binom{n+1}{i+1}.$$

Stirling Numbers

It is convenient to define notation for the entries of the 0^{th} diagonal of the difference table of $h_0, h_1, h_2, \ldots$ for $h_n = n^d$. We let $c(d, i) = \Delta_i h_0$. So that

$$n^d = \binom{n}{0} c(d,0) + \binom{n}{1} c(d,1) + \cdots + \binom{n}{p} c(d,d).$$

The *Stirling Number* $S(d,i)$ *(of the second type)* is defined so that

$$n^d = [n]_0 S(d,0) + [n]_1 S(d,1) + \cdots + [n]_d S(d,d)$$

where $[n]_i = \binom{n}{i} \cdot i!$ is the number of i-permutations of $[n]$.

So $S(d,i) = \frac{c(d,i)}{n!}$. One can show the following. (We skip the proof, but it is in the book).

Theorem 8.2.5. *We have* $S(d,d) = 1$, $S(d,0) = 0$ *for* $d \geq 1$, *and for* $1 \leq k \leq d-1$

$$S(d,k) = kS(d-1,k) + S(d-1,k-1).$$

Theorem 8.2.6. *$S(d,k)$ is the number of ways of partitioning the elements of $[d]$ into k non-empty parts.*

Proof. This is easy using induction. The main argument is that you get such a partionion by adding d to

i. a partition of $[d-1]$ into $k-1$ non-empty parts by adding d into its own part, or

ii. a partition of $[d-1]$ into k non-empty parts by chosing one of the k parts and adding d to it.

□

It follows that $S(d,k) = \frac{1}{k!} S^{\#}(d,k)$ where $S^{\#}(d,k)$ counts the number of ways of partitioning the elements of $[d]$ into k non-empty labelled parts $P_1, \ldots, P_k$.

With this, we can do the following, which is a theorem in the text.

Practice

Use the principle of inclusion-exclusion to show that

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

Conclude that

$$S(d,k) = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^d.$$

The number partitions of $[d]$ into non-empty parts is the *Bell number*

$$B_d = \sum_{k=1}^{d} S(d,k).$$

Note

The *Stirling numbers* $s(d,k)$ *of the first kind* are a dual of the Stirling number of the second kind in that let us write $[n]_d$ in the standard basis:

$$[n]_d = \sum_{k=0}^{d} (-1)^{d-k} s(d,i) n^k.$$

In the text a recurrence relation for them is derived, and they are shown to count the number of ways we can partition $[d]$ into k non-empty circular permutations. This is no more difficult than what we have done, but we skip it, as we will not use them.

8.3 Partition Numbers

We just counted the partitions of distinguishable items into non-empty indistiguishable parts. We have also counted the partitions of indistinguishable items into distinguishable parts: the number of non-negative integer solutions to something like $x_1 + \ldots x_d = n$. We now look a partitioning indistiguishable items into indistiguishable parts.

A *partitition* of a positive integer n is a representation of n as a sum of positive integers. The order of the summands is not important. Let p_n count the number of such partitons of n. For small n we have:

n	partitions of n	p_n
0	$\emptyset$	1
1	1	1
2	2, 1 + 1	2
3	3, 2 + 1, 1 + 1 + 1	3
4	4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1	5

Problem

Looks like Fibonacci! Find p_5.

There are known closed formula for p_n, the first was found by Hardy and Ramanujaun, but they are quite complicated. We do not even have a simple finite recursive formula. In this section we look at generating functions, and branching order n recursions.

Theorem 8.3.1. *The generating function for the sequence* $p_0, p_1, \ldots,$ *of partition numbers is*

$$\sum_{n=0}^{\infty} p_n x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Proof. The choice of a monomial in x^{ik} in

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

corresponds to having i summands k in the partition $a_1 + a_2 + a_3 + \cdots + a_m$ of n. □

Practice

Use the generating function to compute p_5. Why does this not yield a (finite) closed formula for all p_n.

Let $p_n^*(k)$ be the number of partitions of n into at most k parts, and let $p_n^\#(k)$ be the number of partitions of n into exactly k (non-empty) parts.

Practice

Show that $p_n^*(k)$ satisfies the recurrence $p_n^*(k) = p_{n-k}^*(k) + p_n^*(k-1)$. Use this to compute $p_{10}^*(3)$ and $p(5) = p_5^*(5)$.

Practice

Show that $p_n^\#(k)$ of n satisfies the recurrence $p_n^\#(k) = p_{n-k}^\#(k) + p_{n-1}^\#(k-1)$. Use this to compute $p_{10}^\#(4)$

Problem

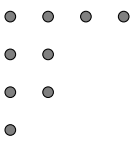
How many ways can you distribute 10 indistinguishable balls among 4 indistiguishable boxes? What if none of the boxes can be empty.

Practice

Let $l_n(k)$ be the number of partitions of n in which no part is smaller than k. Observe that $l_n(n) = 1$ and $l_n(k) = 0$ if $k > n$ (except that we set $l_0(k) = 1$). Show that $l_n(k) = l_n(k+1) + l_{n-k}(k)$ and use it to compute $l_7(3)$ and $p_5 = l_5(1)$.

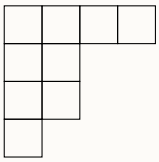
Partitions are often visualised with Ferrer's diagrams.

Example 8.3.2. The partition $9 = 4 + 3 + 1 + 1$ is drawn:

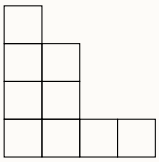


Note

Sometimes it is drawn



or



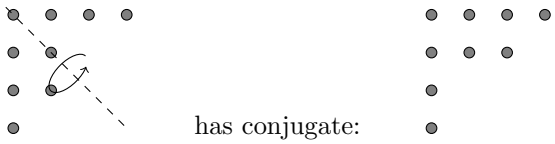
or even

1	3	5	9
2	4		
6	8		
7			

where if the integers are increasing both going down and going right, then it is known as a Young's tableaux.

The *conjugate partition* λ^* of a partion λ is the partiton whose diagram we get by switching rows and columns of (or rotating in 3 dimensions) the Ferrer's diagram

Example 8.3.3. The partition $9 = 4 + 3 + 1 + 1$:



which is $9 = 4 + 2 + 2 + 1$.

Practice

Let $p_n(k)$ be the number of partitions of n in which the largest part has size k. Show that $p_n(k) = p_n^{\#}(k)$.

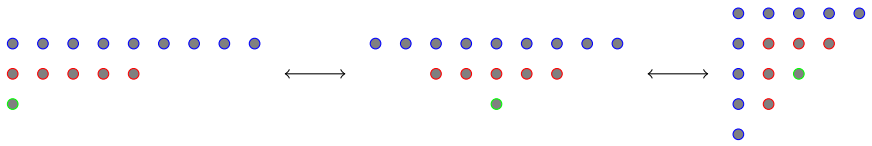
A partition λ is *self-conjugate* if $\lambda = \lambda^*$.

Practice

Find a self-conjugate partition of 10.

Theorem 8.3.4. *Where p_n^s is the number of self-conjugate partitions of n and p_n^t is the number of partitions into* ***distinct odd*** *integers, we have $p_n^s = p_n^t$.*

Proof. We find a one-to-one correspondence. This is one of those proofs where a picture is the best:



□

Problems from the Text

Sect 8.6: 1, 7, 8, 15, 26(a,e), 27,30

Chapter 9

Systems of Distinct Representatives

9.1 General Problem Formulation

The historical presentation of the SDR problem uses the following situation.

There are n women looking for husbands, and m men looking for wives. Each woman i has a list A_i of acceptable men from among the m men. (If a pairing is acceptable for the woman it is also acceptable for the man.) Under what conditions do all the women get married? (There must be a different acceptable man for each woman, when does this happen?)

The mathematical formulation is that there is a set M and a family $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ of subsets of M. A *system of distinct representatives* (SDR) of $\mathcal{A}$ is a n-tuple $(a_1, a_2, \ldots, a_n) \in M^n$ such that

- $a_i \in A_i$ for each $i \in [n]$, and
- $a_i \neq a_j$ if $i \neq j$.

Example 9.1.1. The quadruple $(10, 2, 6, 5)$ is an SDR for the family

$$\begin{aligned} A_1 &= \{5, 10\} \\ A_2 &= \{2, 4, 6, 8, 10\} \\ A_3 &= \{3, 6, 9\} \\ A_4 &= \{5, 10\} \end{aligned}$$

of subsets of $[10]$.

Practice

Determine if SDRs exist for the following familes.

i. $\{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,1\}\}$.

ii. $\{\{1\},\{2,3,4\},\{1,5\},\{8,7,2,4\},\{5,9\},\{9\},\{2,6\}\}$.

iii. $\{\{5,10\},\{5,10\},\{5,10\}\}$.

Practice

The following matrix has several pre-filled 0s.

$$\left[\begin{array}{c|c|c|c} & & 0 & 0 \\ \hline 0 & & & \\ \hline & 0 & 0 & \\ \hline & & & \\ \hline & 0 & 0 & \end{array}\right].$$

You are asked to fill the remaining spaces with 0s and 1s so that

- every column has exactly one 1, and
- every row has at most one 1.

Give a family $\mathcal{A}$ of four subsets of $[5]$ such that there is a placement of 0s and 1s satisfying these conditions if and only if $\mathcal{A}$ has an SDR.

9.2 Existence of SDRs

There is an obvious necessary condition for the existence of and SDR of a family $\mathcal{A}$.

Lemma 9.2.1. *If a family $\mathcal{A} = \{A_1, \ldots, A_n\}$ of subsets of a set M has an SDR, then*

$$\forall I \subset [n] \qquad |\bigcup_{i \in I} A_i| \geq |I|. \tag{MC}$$

The condition (MC) is called the *marriage condition*. Not only is it necessary, it is sufficient.

Theorem 9.2.2. *A family $\mathcal{A} = \{A_1, \ldots, A_n\}$ of subsets of a set M has an SDR if and only if (MC) holds.*

Proof. By the lemma, it is enough to show just the 'if' part. Our proof is by induction on n. If $n = 1$ the theorem is that there is an SDR if and only if A_1 contains an element. This is clearly true. Assume then that the theorem holds for all familes of at most $n-1$ subsets of S and that $\mathcal{A}$

satisfies (MC). There are two cases to consider.

Case 1) If the stronger condition (MC+) holds

$$\forall I \subsetneq [n] \qquad |\bigcup_{i\in I} A_i| \geq |I|+1,$$

then choosing any element $a_n \in A_n$, let $A_I^* = A_i \setminus \{a_n\}$ for all $i < n$. The family $\{A_1^*, \ldots, A_{n-1}^*\}$ is a family of subsets of $S \setminus \{a_n\}$ and so has a SDR $(a_1, \ldots, a_{n-1})$ by induction. This is also an SDR of $\{A_1, \ldots, A_{n-1}\}$, and $(a_1, \ldots, a_n)$ is an SDR of $\mathcal{A}$.

Case 2) If (MC+) doesn't hold, then there is some $I \subsetneq [n]$ such that

$$|\bigcup_{i\in I} A_i| = |I|.$$

We may assume, by reordering $\mathcal{A}$ that $I = \{1, \ldots, t\}$ for some $t < n$. By induction there is an SDR $(a_1, \ldots a_t)$ of $\{A_1, \ldots, A_t\}$. Let $S' = S \setminus \{a_1, \ldots, a_t\}$ and for each $i \geq t$ let $A_i' = A_i \cap S'$. Then $\mathcal{A}' = \{A_{t+1}', \ldots, A_n'\}$ is a family of subsets of S' and we have for any $J \subset \{t+1, \ldots, n\}$ that

$$\begin{aligned} |\bigcup_{i\in J} A_i'| &\geq |\bigcup_{i\in [t]\cup J} A_i| - t \\ &\geq |I \cup J| - t \\ &= |I| + |J| - t = |J|. \end{aligned}$$

Thus there is an SDR $(a_{t+1}, \ldots, a_n)$ of $\mathcal{A}'$ and so $(a_1, \ldots, a_n)$ is an SDR of $\mathcal{A}$. □

Practice

A company is looking to fill 7 jobs $1, \ldots, 7$. There are eight applicants $X_1, \ldots, X_8$ and for $i \in [8]$ applicant X_i is qualified for the jobs in A_i where

$$A_1 = \{3,4,5\}, A_2 = \{3,4,6\}, A_3 = \{2,3,6,7\}, A_4 = \{6\}$$
$$A_5 = \{5,6\}, A_6 = \{4,5\}, A_7 = \{1,3,5,7\}, A_8 = \{3\}$$

Can the company fill all the jobs? How many can be filled?

The following might be useful in the previous question. It is proved in the text as Corollary 9.2.4.

Theorem 9.2.3. *Let $\mathcal{A} = \{A_1, \ldots, A_n\}$ be a family of subsets of a set M. The largest number of sets in a subfamily of $\mathcal{A}$ that has an SDR is the smallest value of*

$$|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}| + n - k$$

over all $k \in [n]$ and all choices of $1 \leq i_1 < i_2 < \cdots < l_k \leq n$.

9.3 Stable Marriages

We change the marriage problem. Now we have n men $m_1, m_2, \ldots, m_n$ and n women $w_1, \ldots, w_n$. All of them will be matched up. Now though, each woman ranks the men in the order of how much she likes them. Woman w_i has an ordering:

$$m_4 >_{w_i} m_7 >_{w_i} \cdots >_{w_i} m_3.$$

Then men rank the women. A *complete marriage* is any matching of the women to the men, but some are better than the others.

For example, we have three women A(ngie), B(etty) and C(lara) and three men X(avier), Y(an) and Z(ack). They rank each other as

$$\begin{array}{lll} Y >_A X >_A Z & Y >_B Z >_B X & Y >_C Z >_C X \\ A >_X C >_X B & A >_Y B >_y C & C >_Z B >_Z A \end{array}$$

Now

$$A \leftrightarrow X \qquad B \leftrightarrow Y \qquad C \leftrightarrow Z$$

is a complete marriage, but how good is it?

It is not stable. Angie prefers Yon to here pair Xavier, and Yon prefers Angie to his pair Betty. This is a dangerous situation. A better complete marriage would be

$$A \leftrightarrow Y \qquad B \leftrightarrow X \qquad C \leftrightarrow Z$$

Betty is less happy, she gets her last choice, but everyone else prefers how they have to Betty, so the will not dilly-dally. This marriage is stable. There are other stable marriages. How do we find one? Let's define stable first.

Note

I define a *stable marriage problem* as a set M of n men and a set W of n women along with a ranking, by each element, of the other set. Though I will use this notation, for exercises you should know the notation the text uses. They describe a problem with a *preferential ranking matrix* $R = [(a_{ij}, b_{ij})]$ where a_{ij} is the rank of man m_j in woman w_i's list, and b_{ij} is the rank of woman w_i in man m_j's list. An example makes it less confusing. The text exprsses the problem

$$\begin{array}{lll} Y >_A X >_A Z & Y >_B Z >_B X & Y >_C Z >_C X \\ A >_X C >_X B & A >_Y B >_y C & C >_Z B >_Z A \end{array}$$

by

$$\begin{array}{c} \\ A \\ B \\ C \end{array} \begin{array}{c} \begin{array}{ccc} X & Y & Z \end{array} \\ \begin{bmatrix} 2,1 & 1,1 & 3,3 \\ 3,3 & 1,2 & 2,2 \\ 3,2 & 1,3 & 2,1 \end{bmatrix} \end{array}$$

Note

'Rank' is tricky in English. The best one is 'highest ranked' and is also 'Rank 1'. When we are talking rank, we say 'high' for the 'low' numbers.

A marriage is *unstable* if there are women w and w' and men m and m' such that

- $w \leftrightarrow m$ and $w' \leftrightarrow m'$, and
- $m' >_w m$, and
- $w >_{m'} w'$.

depicted

$$\begin{array}{ccc} m' & >_w & m \\ \updownarrow & & \updownarrow \\ w' & <_{m'} & w \end{array}$$

A marriage is *stable* if it is not unstable.

9.3.1 The Deferred Acceptence Algorithm for the stable marriage problem

We give an algorithm to find a stable marriage in the stable marriage problem. We then prove that it works. In this algorithm women will ask several men to marry them. If the man accepts, the woman is happy. However, the man may change his mind, and break the engagement if something better comes along.

We start with no matches.

i. While there is an unmatched woman, choose an unmatched woman and have here propose to the highest ranked man that she has not rejected her. (Even if he is matched.)

ii. When a man is proposed to he accepts of the woman who proposed is the highest ranked woman who has proposed to him -they become matched. (He breaks any match that he currently has, the woman becomes unmatched.)

To see that this algorithm finished we observe that a woman always goes down here list, so she can make at most n proposals. If any woman is unmatched in the end, she has asked all men, so every man gets a proposal. Once a man gets a proposal, they are matched and remain matched, so all men will be matched. So all women will be matched too.

To see that the perfect marriage that we end up with is stable, assume that it is not. So there exist $w, w' m$, and m' with

$$\begin{array}{ccc} m' & >_w & m \\ \updownarrow & & \updownarrow . \\ w' & <_{m'} & w \end{array}$$

Since $m' \leftrightarrow w'$, m' was only proposed to by w' or women that he likes less. But w would have proposed to m' before she proposed to m, as she prefers him. This is a contradiction, and so the marriage is stable.

Let's see the algorithm in action.

Example 9.3.1. Consider the problem:

$$w_1 : m_1 > m_3 > m_2 > m_4$$
$$w_2 : m_2 > m_1 > m_4 > m_3$$
$$w_3 : m_3 > m_4 > m_1 > m_2$$
$$w_4 : m_2 > m_1 > m_3 > m_4$$

$$m_1 : w_1 > w_3 > w_2 > w_4$$
$$m_2 : w_1 > w_3 > w_4 > w_2$$
$$m_3 : w_2 > w_3 > w_1 > w_4$$
$$m_4 : w_1 > w_3 > w_4 > w_2$$

Now

- w_1 proposes until m_1 accepts.
- w_2 proposes until m_2 accepts.
- w_3 proposes until m_3 accepts.
- w_4 proposes until m_2 accepts. He breaks his match with w_2.
- w_2 continues from m_1 and proposes until m_4 accepts.

We have a stable marriage, but it is not the only one.

Practice

Solve the same problem, but have the men propose and the women accept or reject. Do you get the same marriage?

A stable marriage is *optimal for women* if each woman gets their highest ranked (favorite) man over all men that they get in any stable marriages.

Theorem 9.3.2. *The deferred acceptance algorithm in which women propose produces a stable marriage which is optimal for women.*

Proof. Call a man m *feasible* for a woman w if he is matched with that woman in some stable marriage. We will show that no man m who is feasible for w will reject her. This is enough.

Indeed towards contradiction, assume that m is feasible for w but rejects her for w'; further assume that this is the first such occerence in the algorithm. As m rejects w we have $w' >_M w$. As it is the first time that a man has rejected a woman that he is feasible for, w' has not proposed to any other feasible men, so the only other men m' that are feasible for w' have $m >_{w'} m'$. As m is feasible for w there is a stable marriage with $w \leftrightarrow m$. In this marriage, $w' \leftrightarrow m'$ for some feasible man other than m, and so we have:

$$\begin{array}{ccc} m' & >_w & m \\ \updownarrow & & \updownarrow, \\ w' & <_{m'} & w \end{array}$$

which does not happen is a stable marriage.

□

Problems from the Text

Section 9.4: 5, 6, 7, 8, 9, 17, 19, 20, 23

Chapter 10

Combinatorial Designs

In this chapter we look at Block Designs. These are families of subsets of a set X, which we usually take to be $\{0, 1, 2, \ldots, v-1\}$ that have tight properties about the number of times different combinations of elements occur together. They arose originally, it seems, out of statistical testing, and the notation reflects this. We call the elements of X varieties rather than points or vertices. We say blocks rather than sets. The designs tend to be hard to build, depending on the necessary parameters. We will look at necessary conditions on the parameters for their existence, and then show some easy constructions of them. Constructions tend to be algebraic, and also arise from structures in such areas as number theory and finite geometry. Those that we will see will depend moslty on Modular arithmetic. I expect you have seen it, so we just give a quick review.

10.1 Modular Arithmetic

For an integer n, the *integers modulo* n, denoted $\mathbb{Z}_n$ is the quotient ring of the integer ring $\mathbb{Z}$ modulo the subring $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. This means that $\mathbb{Z}_n$ contains the elements $\{0, 1, 2 \ldots, n-1\}$ and every integer has a unique *image mod* n via the quotient homomorphism: the image modulo n of an integer x, denoted $x \mod n$, is the unique b in the set $\mathbb{Z}_n$ such that $x = cn + b$ in $\mathbb{Z}$ for some integer c. (Recall that such b exists and is unique by the Division Algorithm.)

For example $17 \mod 5 = 2$. Also $12 \mod 5 = 2$. We write

$$\ldots 17 =_5 12 =_5 7 =_5 2 =_5 -3 \ldots$$

We view 17 as simply a 'nickname' for the element $2 \in \mathbb{Z}_5$.

The ring $\mathbb{Z}_n$ has addition and multiplication operations inherited from $\mathbb{Z}$. For example $2 \times 4 = 3$ in $\mathbb{Z}_5$. We see this by evaluating first in $\mathbb{Z}$ and then taking an image mod 5: $2 \times 4 = 8 =_5 3$. To differentiate these operations from the operations in $\mathbb{Z}$ we sometimes write them as $\oplus$ and $\otimes$. So we will say that in $\mathbb{Z}_5$,

$$7 \oplus 4 = 7 + 4 =_5 1.$$

Practice

In $\mathbb{Z}_{13}$ compute the following.

i. 25

ii. $2 \otimes 5 \oplus 7$

iii. $27 \otimes 25$

iv. $3 \ominus 9$

10.1.1 When $\mathbb{Z}_n$ is a field

Hey! What is '$\ominus$'? Every element a in $\mathbb{Z}_n$ has an *additive inverse* b such that $a \oplus b =_n 0$. It is easy to see that the additive inverse of an element a is unique, and we denote it by $-a$. This is appropriate as clearly $-a \mod n$ is the additive inverse of a. So -4 in $\mathbb{Z}_5$ is the element 1. As shorthand, we write $7 \ominus 4$ for $7 \oplus -4 =_5 7 \oplus 1 =_5 = 1 =_5 3$.

The same is not always true of multiplicative inverses. A *multiplicative inverse* of an element a in $\mathbb{Z}_n$ is an element a^{-1} such that $a \otimes a^{-1} =_n 1$.

Practice

Find a multiplicative inverse of 3 in $\mathbb{Z}_5$. Find one in Z_6.

Yeah. They don't always exist. When do they? Look at the multiplication tables of $\mathbb{Z}_5$ and $\mathbb{Z}_6$:

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	3	1
3	0	3	1	4	2
4	0	4	3	2	1

$\otimes_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Practice

In $\mathbb{Z}_6$ which elements have multiplicative inverse? For what n does every element of $\mathbb{Z}_n$ have a multiplicative inverse.

I expect you have seen the Euclidean algorithm for finding the *greatest common divisor* $\gcd(m, n)$ of two integers m and n, and the Extended Euclidean Algorithm for finding integers a and b such that $am + bn = \gcd(m, n)$.

Practice

Use the Euclidean Algorithm to find $\gcd(96, 25)$. Use the Euclidean Algorithm to find $25^{-1} \bmod 96$ if it exists.

Practice

Show that if there an integers a and b such that $an + bm = d$, then $\gcd(m, n)$ divides d. Conclude that $\gcd(m, n) = 1$ if an only if there exist integers a and b such that $am + bn = 1$.

Use this to prove the following.

Theorem 10.1.1. *An integer m has a multiplicative inverse modulo n if and only if $\gcd(m, n) = 1$. So all elements of $\mathbb{Z}_n$ have multiplicative inverses if and only if n is prime.*

10.2 Block Designs

How many 3-element subsets of the set $S = [7]$ do we need so that every pair of elements of S is in at least one subset?

Well, as any 3-element subset has $\binom{3}{2} = 3$ pairs, and there are $\binom{7}{2} = 21$ such pairs all together, we need at least $21/3 = 7$ subsets. But is this enough? Can you find 7 such subsets? Yep:

$$\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}\{0, 4, 5\}, \{1, 5, 6\}, \{0, 2, 6\}.$$

We ask the question in more generality. Given a set X of v elements (or *varieties*, let $\mathcal{B} = \{B_1, \ldots, B_b\}$ be a collection of k-subsets of X, called *blocks*. It is a em balanced block design if every pair in $\binom{X}{2}$ occurs in exactly λ blocks. If $k = v$, (an uninteresting case) then the design is called complete. If $k < v$ then it is a balanced *incomplete* block design, or BIBD.

A block design can be represented by an incidence matrix. The BIBD with $v = 7, k = 3, b = 7, \lambda = 1$ above has $b \times v$ incidence matrix

	0	1	2	3	4	5	6
B_0	1	1	0	1	0	0	0
B_1	0	1	1	0	1	0	0
B_2	0	0	1	1	0	1	0
B_3	0	0	0	1	1	0	1
B_4	1	0	0	0	1	1	0
B_5	0	1	0	0	0	1	1
B_6	1	0	1	0	0	0	1

Now: given b, k, v, λ, does there exist a BIBD with these parameters?

Practice

Show that every variety must occur in the same number

$$r := \frac{\lambda(v-1)}{k-1}$$

blocks in a BIBD.

There are some necessary conditions for the existence of a BIBD with parameters b, v, k, λ.

i. $2 \leq k < v$. ($k < v$ by definition.)

ii. $r = \frac{\lambda(v-1)}{k-1}$ must be an integer.

iii. $bk = vr$

iv. $\lambda < r$

v. $v \leq b$.

Practice

Prove the first four conditions.

The last condition is not so obvious. It is called Fisher's Inequality. We prove it with some linear algebra. Observe that the dot-product of an column with itself counts the number of times the corresponding variety occurs, so is r. The dot product of a column with another column counts the number of times pairs the corresponding varieties occur in, so is λ. Thus

$$|A^T A| = \begin{vmatrix} r & \lambda & \lambda & \lambda \\ \lambda & r & \lambda & \lambda \\ \lambda & \lambda & r & \lambda \\ \lambda & \lambda & \lambda & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \lambda \\ \lambda - r & r - \lambda & 0 & 0 \\ \lambda - r & 0 & r - \lambda & 0 \\ \lambda - r & 0 & 0 & r - \lambda \end{vmatrix} = \begin{vmatrix} r + 3\lambda & \lambda & \lambda & \lambda \\ 0 & r - \lambda & 0 & 0 \\ 0 & 0 & r - \lambda & 0 \\ 0 & 0 & 0 & r - \lambda \end{vmatrix}$$

As $\lambda < r$ we have that $A^T A$ is non-singular. Thus it has rank v and then so does A. But A is a $b \times v$ matrix, and so $b \geq v$.

We have neccessary conditions for the existence of a BIBD with parameters v, r, k and λ. Are these also sufficient? Far from it. But we will show some examples of BIBD.

10.2.1 SBIBD

When $b = v$ we say that the block design is *symmetric*, and call it an SBIBD. When $b = v$ we see that

- $k = r$.

- $\lambda = \frac{k(k-1)}{v-1}$.

The example for $v = 7$ and $k = 3$ that we saw above above can be constructed from the first block

$$B_0 = \{0, 1, 3\}$$

by letting $B_i = B_0 + i = \{0+i, 1+i, 3+i\}$. Clearly each variety occurs in three blocks (once as the first element, once as the second, and once as the third. To see that every pair occurs, it is enough now to observe that every difference in $\{1, 2, 3, 4, 5, 6\}$ occurs once as a difference $i - j$ between two of the elements i and j in B_0. The set B_0 is called a difference set.

Practice

Show that $\{0, 1, 2, 6, 9\}$ is a difference set. It can be used to construct a SBIBD with what parameters?

Practice

Show that if there is a BIBD with parameters b, k, v, r and λ then there is one with parameters cb, k, v, cr and $c\lambda$ for every integer $c \geq 1$.

10.3 Steiner Triple system

A BIBD with $k = 3$ and $\lambda = 1$ is called a Steiner Triple System or STS(v).

Practice

Show that an STS(v) has $r = (v-1)/2$ and $b = (v^2 - v)/6$. Use this to prove Fact 10.3.1.

Fact 10.3.1. *An* STS(v) *can exist only if* $v =_6 1, 3$.

On the other hand, the following is true.

Theorem 10.3.2. *If v is an integer greater than 1 with $v =_6 1, 3$, then there is an* STS(v).

We will not prove this completely, but we will show how to construct infinitely many STS.

Lemma 10.3.3. *Where X_u and $\mathcal{B}_u$ are the sets of varieties and blocks of the* STS(u) *and X_v and $\mathcal{B}_v$ are the sets of varieties and blocks of the* STS(v), *let*

$$X = X_u \times X_v = \{(a, b) \mid a \in X_u, b \in X_v\}$$

and let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$ where

- $\mathcal{B}_1 = \{\{(a_1, b), (a_2, b), (a_3, b)\} \mid \{a_1, a_2, a_3\} \in \mathcal{B}_u, b \in X_v\}$,

- $\mathcal{B}_2 = \{\{(a,b_1),(a,b_2),(a,b_3)\} \mid a \in X_u, \{b_1,b_2,b_3\} \in \mathcal{B}_v\}$, *and*
- $\mathcal{B}_3 = \{\{(a_1,b_1),(a_2,b_2),(a_3,b_3)\} \mid \{a_1,a_2,a_3\} \in \mathcal{B}_u, \{b_1,b_2,b_3)\} \in \mathcal{B}_v\}$.

$\mathcal{B}$ *is an* STS(uv).

Proof. We show that every pair $(a,b),(a',b')$ of distinct vertices occurs together in exactly one block. Indeed, if $a = a'$ then the pair can only occur in $\mathcal{B}_1$. In this case we have that $b \neq b'$ as the vertices (a,b) and (a',b') are distinct. The pair (b,b') therefore occurs in a unique block in $\mathcal{B}_u$ and so $(a,b),(a',b')$ in a unique block in $\mathcal{B}_1$. The proof in the case $b = b'$ is similar. So we may assume that $a \neq a'$ and $b \neq b'$. Then the pair can only occur in $\mathcal{B}_3$. Again, the pair (a,a') occurs in a unique block (a_1,a_2,a_3) in $\mathcal{B}_u$ and (b,b') occurs in a unique block (b_1,b_2,b_3) in $\mathcal{B}_v$. □

Now as, we already have an STS(3) and an STS(7). The above lemma implies that we have STS(v) for any v whose prime factorisation contains only 3s, and 7s.

Practice

Construct an STS(21).

Practice

In the proof of the lemma, how many blocks are in $\mathcal{B}_1, \mathcal{B}_2$ and $\mathcal{B}_3$? (Careful for $\mathcal{B}_3$; blocks are unordered, so a given $\{a_1,a_2,a_3\} \in \mathcal{B}_u$ and $\{b_1,b_2,b_3)\} \in \mathcal{B}_v$ produce more than one block in $\mathcal{B}_3$.)

Show that the sum of these is equal to $((uv)^2 - (uv))/6$.

How can you use this to simplify the proof?

10.4 Latin Squares

A *latin square of order* n is an $n \times n$ matrix A with entries in $\mathbb{Z}_n$ such that each integers occurs exactly once in each row and in each column.

Here are a couple of latin squarea of order 5

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

Note

Recall that in a matrix $M = [m_{ij}]$, m_{ij} is the entry in the i^{th} row (i down) and j^{th} column (j over).

Writing them out like this is good for understanding, but a bit unwieldy. The first can be denoted as $A = [a_{ij}]$ where $a_{ij} = i + j \mod 5$. (It is the $\oplus$ table for addition modulo 5.)

Practice

Express the second latin square $B = [b_{ij}]$ in a similar way.

It should be clear that for any latin square of order n we get another by permuting the entries. We can always permute entries of a latin square so that the first row is $0, 1, \ldots, n-1$. A latin square with this first row is in *standard form*.

Practice

For each n define a latin square of order n in standard form. Can you construct another?

That's too easy. Two different latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ of order n are *orthogonal* if for each pair $(a, b) \in \mathbb{Z}_n^2$ there is an i and j such that $a_{ij} = a$ and $b_{ij} = b$. Those pictured above are orthogonal. In a pair of orthogonal latin squares (or POLS), we can of course assume that one of them is in standard form. But actually, permuting the elements of the second latin square will no change the fact that is is orthogonal, so, we can assume both are in standard form.

You've hopefully already observed that there are no POLS of order 2.

Practice

Find a pair of orthogonal latin squares of order n for any every odd n

There are usually many. In fact, a set of latin squares of order n is a set of *MOLS*, for 'Mutually Orthogonal Latins Squares' if every pair of latin squares in the set is a POLS.

Practice

Show there cannot be a set of more than $n-1$ MOLS of order n.

Practice

Show that if n is a prime there is a set of $n-1$ MOLS of order n.

What about non-primes n. It can be shown that there are $n-1$ MOLS of order n if $n = p^d$ for some prime p, but we will not do this. But how about, say, $n = 6$. The following is not so easy. It was proved in 1901 by Tarry.

Theorem 10.4.1. *There is no pair of orthogonal latin squares of order* 6.

Euler conjectured in about 1760 there are no POLS of order n for any $n =_4 2$. He was wrong. In fact there are POLS of order n for all $n \neq 2, 6$. This follows by finding POLS of orders 9 and $2k$ for all odd $k \geq 5$, (which we will not show) and the following theorem.

Theorem 10.4.2. *If there is a pair POLS of order m and a POLS of order n, then there is a POLS of order mn.*

Proof. The proof is based on the followng construction. For a latin square $A = [a_{ij}]$ of order m and a latin square $B = [b_{ij}]$ of order m let $A \oplus B$ be the matrix of order mn whose ij^{th} entry is defined as follows. Observe that the numbers in mn can be enumerated as $i \cdot n + i'$ for $i \in [m]$ and $i' \in [n]$. (Indeed $a = i \cdot n + i'$ where $i' = a \mod n$ and $i = (a - i')/n$, but this isn't so important.) The $(in + i', jn + j')$ entry of $A \oplus B$ is the pair $(a_{ij}, b_{i'j'})$.

Where $\{A, A'\}$ is a POLS of order m and $\{B.B'\}$ is a POLS of order n, we claim that $\{A \oplus B, A' \oplus B'\}$ is a POLS of order mn.

It is enough to show that each pair $(a, b), (a', b') \in \mathbb{Z}_m \times \mathbb{Z}_n$ occurs for some $in + i'$ and $jn + j'$. Well, the pair (a, a') occurs for some i, j; that is, $a_{ij} = a$ and $a'_{ij} = a'$. Similarily, there are i' and j' such that $b_{i'j'} = b$ and $b'_{i'j'} = b'$. So the $(in + i', jn + j')$ entry of $A \oplus B$ is $(a_{ij}, b_{i'j'}) = (a, b)$ and of $A' \oplus B'$ is $(a_{i'k'}, b_{i'j'}) = (a', b')$. This is what we needed to show. □

Practice

Using the constuction in the proof, find

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}.$$

A set of $n - 1$ MOLS of order n can be used to make a BIBD with parameters $b = n^2 + n, v = n^2, k = n$ and $\lambda = 1$.This is done in some detail in the text, but we just show a simple example with $n = 3$, which gives us a STS(9).

Consider the POLS

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \text{ and } A' = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}.$$

Our set of varieties is $[n]$ we write them as follows:

$$\begin{bmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{bmatrix}.$$

Our twelve 3- blocks are of four types:

i. Rows: $\{0, 1, 2\}$, $\{3, 4, 5\}$, and $\{6, 7, 8\}$.

ii. Columns: $\{0,3,6\}\{1,4,7\}$, and $\{2,5,8\}$.

iii. Triples of positions with the same i in A: $\{0,5,7\},\{1,3,8\}$, and $\{2,4,6\}$.

iv. Triples of positions with the same i in A': $\{0,4,8\},\{2,3,7\}$, and $\{1,5,6\}$.

Practice

Argue that this is an STS.

Problems from the Text

Sect. 10.5: 1, 2, 10, 20, 21, 28, 29,39, 50

Chapter 11

Intro to Graph Theory

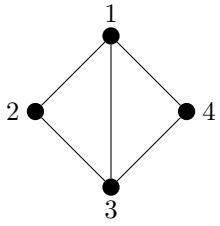
11.1 Basic Definitions

Definition 11.1.1. A graph $G = (V, E)$ consists of a non-empty set V of *vertices* and a set E of 2-element subsets of V, called *edges.*

For example

$$G = (\{1, 2, 3, 4\}, \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}, \{1, 3\}\})$$

is a graph. It has four vertices and five edges. As this mess of brackets gets troublesome to write, we drop them when it doesn't confuse things an write an edge $\{x, y\}$ as xy. The graph G can be represented pictorially as one of



We often write $V(G)$ for V and $E(G)$ for E if we don't define the these sets for a graph G explicitly.

There are a lot of definitions related to the fact that $e = uv$ is an edge of G. We say

- the vertices u and v are *adjacent*, written $u \sim v$,
- u and v are *neighbours*,
- u and v are the *endpoints* of e,

- u (and v) is incident with e,

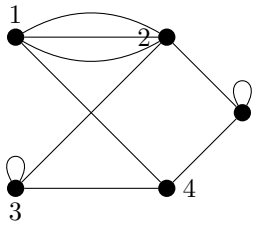
Practice

What is the maximum number of edges in a graph on n vertices?

Practice

How many different graphs are there on the vertex set $[n]$?

A *general graph* is like a graph, except we allow E to be, and to contain, multisets. That is, it may have multiedges and loops:



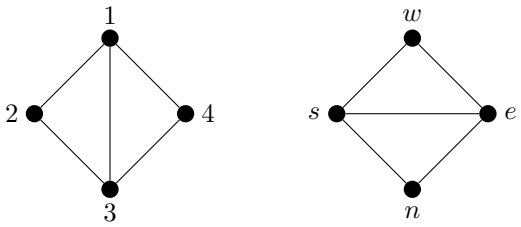
The *multiplicity* of an edge is the number of times it occurs.

Definition 11.1.2. An *isomorphism* is a bijective map $f : V(G) \to V(H)$ such that

$$uv \in E(G) \iff f(u)f(v) \in E(H).$$

If there is an isomorphism f from G to H, we say G and H are *isomorphic*, and write $G \cong H$.

Example 11.1.3. The following graphs are isomorphic



Practice

How many non-isomorphic graphs are there on 4 vertices?

Practice

What is the isomorphism?

If two graphs are isomorphic, we usually consider them the same, and so the vertices can be given convenient names, an a graph can often be defined with just a picture.

Some common graphs are:

- The complete graph on n vertices, K_n, has $V(K_n) = [n]$ and $E(K_n) = \{ij \mid 1 \leq i < j \leq n\}$.
- The n-cycle, C_n, has $V(C_n) = [n]$ and $E(C_n) = \{i(i+1) \mid i = 1, \ldots, n-1\} \cup \{n1\}$.
- The n-path, P_n, has $V(P_n) = \{0, 1, \ldots, n\}$ and $E(P_n) = \{i(i+1) \mid i = 0, \ldots, n-1\}$.
- The complete bipartite graph, $K_{m,n}$, has $V(K_{m,n}) = \{a_1, \ldots a_m\} \cup \{b_1, \ldots, b_n\}$ and $E(K_{m,n}) = \{a_i b_j \mid i \in [m], j \in [n]\}$.
- The n-cube, Q_n, $V(Q_n)$ is the set of binary strings of length n, vertices u and v are adjacent if they differ in exactly one coordinate.

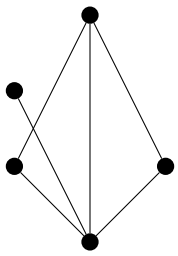
Practice

Draw these graphs. (For n upto some reasonable number.)

It is a hard problem to decide if two (reasonably large) graphs are isomorphic. But there are several invariants that are easy to calculate, that can help us show that two graphs are not isomorphic.

The *degree* $\mathrm{d}(v)$ of the vertex v in a graph is the number of edges it is in, (plus the number of loops). A list of the degrees of the vertices of a graph in non-ascending order is the degree sequence.

Example 11.1.4. The graph



has degree sequence $(4, 3, 2, 2, 1)$,

Practice

What are the degree sequences of K_n and C_n?

Notice that not any non-increasing seqeunce of integers is the degree sequence of a graph. Every edge of the graph contributes two to degrees in the sequence, so a degree sequence must sum to an

even number. This leads to a simple observation that is known as the hand-shaking Lemma: Every graph has an even number of odd degree vertices.

The degree sequence is a graph invariant– isomorphic graphs have the same degree sequences, so if two graphs have different degree sequences we know they are different. Lets find some more graph invariants.

Given a graph G, another graph G' is a *subgraph* of G, written $G' \leq G$ if $V(G') \subset V(G)$ and $E(G') \subset E(G)$.

A subgraph G' of G is *spanning* if $V(G') = V(G)$, or *induced* if $E(G') = \{uv \in E(G) | u, v \in V(G')\}$. A subgraph G' of G is a *proper* subgraph of G if $E(G')$ is a proper subset of $E(G)$.

Let x and y be vertices in a graph G. A *walk* in a graph G is a finite alternating sequence of vertices and edges:

$$x_0, e_1, x_1, e_2, e_2, \ldots, x_{n-1}, e_n, x_n$$

where $e_i = x_{i-1}x_i$ for $i = 1, \ldots n$.

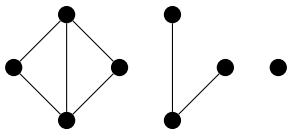
Usually we just write the vertices

$$x_0 x_1 \ldots x_n.$$

The *length* of the walk is n, the number of edges in it. It is a *trail* if the edges are distinct, a *path* if the vertices are distinct. The first and last vertices are the *endpoints* of the walk, and if they are x and y respecively, we call the walk an xy-walk. A walk is *closed* if its endpoints are the same vertex. The distance (x, y) between two vertices in G is the length of the shortest xy-walk in G.

A graph G is *connected* if for every $x, y \in V(G)$ there is an xy-walk in G. A maximally connected subgraph of G is a component of G.

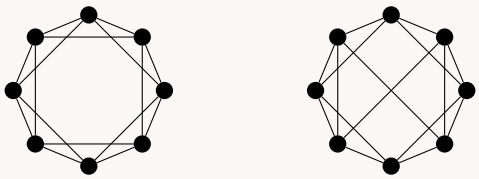
Example 11.1.5. This graph has 3 components.



The connectedness or number of components of a graph is clearly an invariant. So is the number of copies of a given subgraph.

Practice

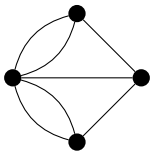
Are the following graphs isomorphic?



11.2 Eulerian Trails

It is often told that the first problem of graph theory was the problem of the Bridges of Königsberg. In the fictional city of Königsberg (Problem: prove or disprove my unpopular claim that Königsberg is fictional.) there were seven bridges. The dandies of the city, on slow Sunday, would walk about the town, playing a riddlish game. Starting whereever they pleased, they were to walk around, crossing every bridge, without crossing any bridge more then once. This game went on for centuries, and several liars claimed to have done it. Fermat once wrote in the margin of a book that it was simple enough. Until eventually, Euler proved it was impossible, and stabbed Fermat in a dual. (Prove that any of this is true.)

The city of Königsburg consisted of four dots, connected by seven bridges. It looked a lot like this:



How Euler proved it is lost in the depths of historical fiction. But our story inspires the following definitions.

Definition 11.2.1. A trail in a graph G is an *euler trail* if it contains every vertex (possibly several times), and contains every edge (exactly once). If it is closed, then it is an *euler circuit*. A graph is *eulerian* if it contains an euler circuit.

The following is what Euler claims to have proved.

Theorem 11.2.2. *A graph is eulerian if and only if it is connected and all of its vertices have even degree.*

Proof. That an eulerian graph must be connected is super clear. That all vertices have even degree is pretty clear: Let $C = v_1 v_2 \dots v_N$ be an eulerian circuit. For any vertex v, count the number of times d that v occurs in $v_1 v_2 \dots v_{N-1}$. For each occurence $v = v_i$ is in two edges in C: $v_{i-1}v$ and vv_{i+1}. So v is in $2d$ edges in C. But C has exactly the same multiset of edges as G, so is in $2d$ edges in G.

Now, in the other direction, assume that G is a connected graph in which every vertex has even degree. We must show that there is an euler circuit in G. Let $T = v_1 v_2 \dots v_m$ be a longest trail in G.

First observe that T must be closed. Indeed, if it weren't, then the degree of v_m in G is odd by our proof above, so there is another edge in G incident to $T(v_m)$. Adding this to T, we would get a longer trail. So T is a circuit.

If T is not an euler circuit , then $G' = G \setminus T$ is non-empty. As G is connected, there is an edge $e = u_1 u_2 \in G'$ with $u_1 = v_i$ in $V(T)$. Letting $T' = u_1 u_2 \dots u_{m'}$ be a maximal trail in G' that begins

with u_1u_2 we again get that T' must be closed; that is $u_{m'} = u_1 = v_i$. But then

$$v_1v_2 \ldots, v_iu_1u_2 \ldots u_{m'}v_{i+1} \ldots v_m$$

is a trail in G that is longer than T. This is a contradiction, so T must have been an euler circuit. Thus G is eulerian. □

Practice

Give necessary and sufficient conditions for a graph to have an euler trail. Does Königsberg satisfy these conditions?

11.3 Hamilton Paths and Cycles

Recall that a path is a trail in which no vertex is repeated. A *cycle* is a closed path– a circuit in which no vertex is repeated (though when we write it as a path: $v_1v_2v_3v_1$ the endpoint seems to be repeated).

Definition 11.3.1. A path, or cycle, in G is *hamilton* if it contains all vertices of G. A graph G is *hamiltonian* if it contains a hamiltonian cycle.

Practice

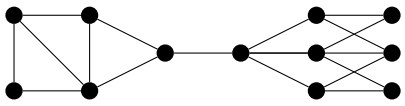
Show that the Petersen graph has a hamilton path but is not hamiltonian?

Practice

Find a hamilton path in Q_n. Does this remind you of something else we did?

There were some nice conditions that characterised the eulerian graphs. We are not so lucky with hamilton graphs. In fact, the problem of deciding if a graph on n vertices is hamiltonian, is NP-complete. This means the best known algorithm we have for deciding, takes time that is exponential in in n, (at least for some graphs). This doesn't mean we can't say anything about graphs that are hamiltonian. Indeed they must be connected, and have no leaves. We can say a bit more.

Example 11.3.2. A graph G with a *bridge*– an edge whose remove disconnects G, cannot have a hamilton cycle;



Practice

Show that there is a non-hamltonian graph on even n vertices with min degree $n/2 - 1$. Show there is a connected sub graph.

Dirac showed that if a graph has min-degree at least $n/2$ then it is hamiltonian. The following theorem of Ore is a slight refinement of Dirac's theorem.

Theorem 11.3.3. *If a graph G of order $n \geq 3$ satisfies Ore's Property*

$$x \not\sim y \Rightarrow \mathrm{d}(x) + \mathrm{d}(y) \geq n \qquad (*)$$

then G has a hamilton cycle.

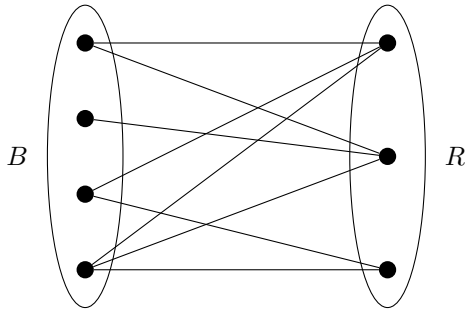
Proof. For fixed $n \geq 3$, assume, towards contradiction, that there are non-hamltonian graphs satisfying (*). Let G be a maximal such graph. As K_n has a hamilton cycle, G is missing some edge. By the maximalily of our counterexample, adding this edge makes a hamiltom cycle, so G contains a hamilton path $v_1, \ldots, v_n$. Now, for each $i \in [n-1]$, either v_1v_{i+1} or v_iv_n is not an edge in G or else we could find a hamilton cycle. So for every neighbour v_i of v_n, v_{i+1} is a non-neighbour of v_1. Thus $\mathrm{d}(v_1) \leq (n-1) - \mathrm{d}(v_n)$. which yields $\mathrm{d}(v_1) + \mathrm{d}(v_n) \leq n - 1$ contradicting (*). □

Problem

Use Ore's theorem to prove Dirac's theorem.

11.4 Bipartite Graphs

A graph $G = (V, E)$ is *bipartite* if there is a partition $V = R \cup B$ of the vertices such that all edges have one endpoint in R and one in B.



A graph is biparite if and only if you can 2-colour it: colour the vertices with the colours red and blue so that no adjacent vertices have the same colour.

Practice

Show that Q_n is bipartite. Show that C_{2n+1} is not bipartite.

Practice

Show that any odd circuit in a graph contains an odd cycle.

Theorem 11.4.1. *A graph is bipartite if and only if it contains no odd cycles.*

Proof. If a graph has an odd cycle, then we cannot 2-colour the cycle, so cannot 2-colour the graph, so the graph is not bipartite.

On the other hand, assume G is not bipartite. Pick a vertex v_0, and colour a vertex v red if (v_0, v) is even or blue if $d(v_0, v)$ is odd. As G is not bipartite, this is not a 2-colouring, so there are adjacent vertices u and v that get the same colour.; wlog red. They both have even distance from v_o, so both have even length paths to v_0. These paths with the edge between u and v make up an odd circuit, which we saw contains an odd cycle. □

Practice

What is the maximum number of edges in a bipartite graph on n vertices?

Practice

Show that any graph with m edges has a bipartite subgraph with at least $m/2$ edges.

11.5 Trees

A graph T is a *tree* if it is connected and contains no cycles. There are several alternate definitions for trees. The equivalence of these definitions is quite clear, though it is a little tedious to prove.

Theorem 11.5.1. *For a graph T on n vertice, the following are equivalent.*

i. *T is a tree.*

ii. *Every edge of T is a bridge.*

iii. *T is connected and it has $n-1$ edges.*

iv. *Every pair of vertices of T is joined by a unique path.*

Problems from the Text

11.8: 1, 3, 5, 13, 20, 54, 66(with proof)

Chapter 12

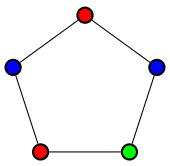
More on Graph Theory

12.1 Graph Colouring

A *(proper vertex-)colouring* of a graph $G = (V, E)$ is a function $f : V(G) \to S$ for some set S such that

$$u \sim v \Rightarrow f(u) \neq f(v).$$

Viewing the different elements of S as colours, a colouring of C_5 looks like this:



We saw in the section on bipartite graphs that a graph has a colouring with two colours if and only if it is bipartite.

A *k-colouring* of a graph G is a colouring $f : V(G) \to [k]$. If G has a k-colouring it is *k-colourable*. The smallest k for which G is k-colourable is the *chromatic number* $\chi(G)$ of G. If $\chi(G) = k$ then G is *k-chromatic*.

Practice

What is the chromatic number of K_n? ...C_n? ...P_n? ...Q_n? ... the Petersen graph?

Practice

Show that chromatic number is a graph invariant. That is, show that isomorphic graphs have the same chromatic number.

Practice

Show that $1 \leq \chi(G) \leq n$ for any graph G on n vertices.

That was too easy. The *maximum degree* $\Delta(G)$ of a graph G is the first degree in its degree sequence. We claim that for any graph G:

$$\chi(G) \leq \Delta(G) + 1$$

Indeed, order the vertices $v_1, \ldots, v_n$ and for $i = 1, \ldots, n$ colour v_i with the lowest integer in $[\Delta + 1]$ not yet used on a neighbour of v_i- as at most Δ colours can be used by neighbours of v_i, this is possible, and it is clearly a colouring of G. This colouring is called a *greedy colouring* of G.

Practice

Show that the bound $\chi(G) \leq \Delta(G) + 1$ is 'tight': that there are graphs for which equality holds. Show also that there are also graphs for which $\chi(G)$ and $\Delta(G) + 1$ can be arbitrarily far apart.

Except in the few tight cases that you observed, one can improve this bound. Brooks showed the following.

Theorem 12.1.1. *If G is a connected graph other than a complete graph or an odd cycle, then $\chi(G) \leq \Delta(G)$.*

A greedy colouring of a graph depends on the ordering $v_1, \ldots, v_n$ of the vertices.

Practice

Show that for every graph G there is an ordering of the vertices such that the greedy ordering colours the graph with $\chi(G)$ colours. Find a 2-chromatic graph and an ordering of the vertices of this graph for which the greedy colouring uses 4 colours.

The proof of this in nice, and not so hard, but it takes some time, and so we follow the text in omitting it.

Problems from the Text

12.8: