Discrete Math for Computing

Working Draft

Contents

Part I: Counting and Relations

Part II: Logic and Proof

Part III: Modular Arithmetic and Cryptography

Part IV: Induction and Recurrences

Part V: Graphs

Part VI: Groups and Codes

1 Counting

There are three types of mathematicians. Those who can count and those who can't.

1.1 Orderings

The details of the question always matter. So always take a second look at what is being asked before leaping.

EXAMPLE 1.1. *Each of twenty students have to present an oral report. In how many orders can this happen?*

The answer is $20 \times 19 \times 18 \ldots \times 2 \times 1$.

The most natural way to calculate this is to say: there are 20 choices for who goes first, 19 choices for who goes next, 18 choices for the third person, and so on.

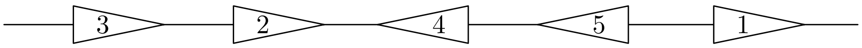
But we can also consider it from the student's perspective. There are 20 slots. There are 20 slots for Adam, then 19 slots for Beth, then 18 slots for Carol, and so on.

The product $20 \times 19 \times 18 \times \ldots \times 1$ is called **20 factorial**, written with an exclamation point as 20!. Note that $1! = 1$. And furthermore, note that $0! = 1$ by definition. (There are good logical reasons why this is the case, mainly that this means that many many formulas still work, but at the end of the day, this is a definition.)

1.2 Sequential Counting

The above is a special case of a general idea in counting: to break up the question into a series of choices. This occurs naturally when counting sequences—a series of objects where the order matters. The idea is that we construct every sequence under consideration by a series of choices. *If we have the same number of options for each choice, then to get the overall number of sequences, multiply the number of options together.*

EXAMPLE 1.2. *A chromosome contains many* **genes**. *The genes do not overlap, and each gene can be oriented either forward or back. For example, we might depict a chromosome with, in order, gene* 3 *forward, gene* 2 *forward, gene* 4 *back, gene* 5 *back, gene* 1 *forward, as follows:*



(a) Given 10 genes, how many possible chromosomes are there, if the 10 genes must appear in order from 1 up to 10?
(b) How many possible chromosomes are there with 10 given genes?

(a) The choices we have are the orientations of the genes. Gene 1 can be oriented forward or back: two choices. Gene 2 can be oriented forward or back: two choices. And so on. So there is a total of 2^{10} possible chromosomes.

(b) The simplest way to do this one, is to first choose the ordering of the genes. There are 10! orderings. Then choose the orientations. So the total is $10! \times 2^{10}$.

EXAMPLE 1.3. *Define a* **word** *as any sequence of letters, such as* `qjgqri`.
(a) How many 5-letter words are there?
(b) How many 5-letter words end in a consonant (non-vowel)?
(c) How many 5-letter words contain no vowel?
(d) How many 5-letter words have all their letters distinct?

(a) We construct the words one letter at a time. We have 26 options for the first letter. Then, we have 26 options for the second letter. And so. Thus the answer is $26 \times 26 \times 26 \times 26 \times 26 = 26^5$.

(b) Again, we construct the words one letter at a time. We have no constraint on any of the first four letters. For the last letter, there are 5 vowels, and so we have 21 options for the last letter. Thus the answer is $26^4 \times 21$.

(c) This time we have 21 options for each letter. Thus the answer is 21^5.

(d) We construct the words one letter at a time. As before, there are 26 options for the first letter. For the second letter, there are 25 options (it cannot be the same as the first letter). Now for the key point: when we reach the third letter, there are 2 forbidden letters; no matter what the first two letters are, they are different. And so there are 24 options here. Thus the answer is $26 \times 25 \times 24 \times 23 \times 22$.

▶ **For you to do!** ◀
1. *How many 5-letter words have a middle letter that is a vowel?*
2. *How many 5-letter words are there whose first and last letter are the same?*
3. *How many 5-letter words are there whose first and last letter are different?*

1.3 The Product Rule and Choosing without Replacement

The fundamental idea for counting discussed above is sometimes summarized by a rules called the **product rule**. The rule is phrased in terms of sets. A **set** is a collection of objects without repeats. The **size** or **cardinality** of a set S is denoted $|S|$ and is the number of elements in the set.

Lemma 1.1 (The Product Rule) *If A and B are sets, then the set of ordered pairs each consisting of one element of A and one element of B is denoted $A \times B$. This has size:*

$$|A \times B| = |A| \times |B|.$$

There is one ordered pair for each element of A and each element of B.

Example 1.4. *Consider a set S with n elements. How many different subsets does S have? (Note that "subset" allows for the possibility of nothing (the empty set) or everything (S itself).)*

The answer is 2^n. We can go through the elements of S one at a time, and for each we have two options: in or out. It is important to note that these choices are independent—one choice does not constrain another.

A common counting situation is what we call **choosing without replacement**: as each item is chosen, it is not resurrected for future choices.

Lemma 1.2 *Consider a universe X of n elements, and $1 \leq k \leq n$.*
(a) The number of ways to choose an ordered sequence of k elements from X with replacement is n^k.
(b) The number of ways to choose an ordered sequence of k elements from X without replacement is $n!/(n-k)!$.

Proof. (a) Each of the k times we have n choices.
(b) The answer, call it A, is the product $n \times (n-1) \times \cdots \times (n-k+1)$. If we multiply A by $(n-k)!$, we therefore obtain $n!$. That is, $A = n!/(n-k)!$. $\diamondsuit$

Note that, because $0!$ is defined as 1, the second formula works even if $k = n$.

Example 1.5. *Consider 4 boys and 5 girls.*
(a) In how many ways can they line up for the bus?
(b) In how many ways can they line up for the bus with a girl in front?
(c) In how many ways can they line up for the bus with no two girls next to each other?

(a) The genders don't matter. There are 9 people. There are 9 options for the person in front, 8 for the next, and so on. The result is $9 \times 8 \times 7 \times \ldots \times 1$, which is $9!$.

(b) We have 5 options for the first person. After that there is no constraint. So the answer is $5 \times 8!$.

(c) The only way this can happen is if we alternate girl, boy, girl, boy, girl, et cetera. We have 5 options for the first girl, 4 options for the first boy, and so on. The answer is $5! \times 4!$.

1.4 Counting by Cases or Complements

Another common idea in counting is to divide up the collection into separate cases. In this approach, we count the individual cases separately and then add the answers we get.

EXAMPLE 1.6. *Suppose we roll two dice. If the dice are distinguishable, how many outcomes are there? What if the dice are indistinguishable?*

Say the dice are distinguishable; for example, one red, one green. Then a red 3 and green 5 is considered different to a green 3 and red 5. So there are simply $6^2 = 36$ possibilities, 6 for each die.

Say the dice are indistinguishable. This means that 3 and 5 is considered the same as 5 and 3. We can count these by focusing on the bigger value: there are 6 outcomes where the maximum is 6, 5 outcomes where the maximum is 5, and so on. So the answer is $6+5+4+3+2+1 = 21$. The pairs are $66, 65, 64, 63, 62, 61, 55, 54, 53, 52, 51, 44, 43, 42, 41, 33, 32, 31, 22, 21, 11$

A variation of this is where we count the collection by its **complement**. That is, we count the collection by counting the whole universe and then subtracting those things that are **not** in our collection.

EXAMPLE 1.7. *How many 5-letter words have at least one vowel?*

Well, we could try to count those with one vowel, those with two vowels, and so on. But it is easier to count those with no vowel and subtract that from the total. We calculated these two quantities in Example 1.3. So the answer is $26^5 - 21^5$.

Some people like to summarize this approach with the sum rule:

Lemma 1.3 (The Sum Rule) *If sets A and B are disjoint (meaning their intersection is empty), then $|A \cup B| = |A| + |B|$. More generally,*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. If we count the elements in A and B, then we get every element in the union $A \cup B$, except that the elements in the intersection $A \cap B$ are counted twice. ◊

We use the product and sum rules all the time in counting, even if we often don't make this explicit.

> ► **For you to do!** ◄
> *4. In the Mighty Math Mob there are* 4 *freshman,* 5 *sophomores,* 6 *juniors, and* 7 *seniors. In how many ways can one form a committee of* 3 *people, no two of whom are in the same year?*

Exercises

1.1. At the local BananaAnts restaurant, there is a special three-course dinner. You choose one appetizer, one entree, and one dessert; there are 3 appetizers, 4 entrees and 5 desserts. How many possible dinners are there?

1.2. Consider South Carolina's license plate, which is three letters followed by a three-digit number. (Leave answers as products.)

(a) How many possible license plates are there if the number must be even?

(b) How many possible license plates are there if no vowels allowed?

(c) How many possible license plates are there if all letters and digits must be distinct?

(d) How many possible license plates are there if we change the rules to allow either 3 or 4 letters?

1.3. An SSN is a 9-digit number with zeroes allowed in every position.

(a) How many SSNs are there all of whose digits are even?

(b) How many SSNs are a multiple of 2?

(c) How many SSNs are there that are palindromes (read the same forward as backwards)?

(d) How many SSNs are there all of whose digits are distinct?

(e) How many SSNs are there such that no two consecutive digits are the same?

(f) How many SSNs are there whose digits are strictly increasing.

1.4. Wendy needs to schedule 10 different speakers at a rally (who each speak exactly once).

(a) How many orderings are there such that Fred speaks after Beth (not necessarily consecutive)?

(b) How many orderings are there such that Fred speaks immediately after Beth?

(c) There are 3 Democrats and 7 Republicans on the list. How many orderings are there with a Democrat as an opening speaker and a Republican as a closing speaker?

1.5. There are six different Welsh books, eight different Xhosa books, and five different Yiddish books.

(a) In how many different ways can these books be arranged on a bookshelf?

(b) In how many ways can these books be arranged on a bookshelf if all books in the same language are grouped together?

1.6. Consider 5-letter words again.

(a) How many start and finish with a vowel?

(b) How many have at most one vowel?

(c) How many have exactly three vowels with no two vowels next to each other?

1.7. Consider 5 boys and 5 girls.

(a) In how many ways can they line up for the bus with a girl in front?

(b) In how many ways can they line up for the bus with both a girl in front and at the back?

(c) In how many ways can they line up for the bus with a girl in front or at the back or both?

(d) In how many ways can they line up for the bus with no two girls next to each other?

1.8. A **pandigital** number is a 9-digit number all of whose digits are different and containing no zero. (For some of these, it might be quicker to write some code.)

(a) How many pandigital numbers are there?

(b) How many pandigital numbers are even?

(c) How many pandigital numbers are perfect squares?

(d) How many pandigital numbers are prime numbers?

1.9. Prove the following generalization of the Sum Rule: For all sets A, B, C,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

1.10. If we write out 30!, how many zeroes are there at the end?

Solutions to Practice Exercises

1. There are 5 choices for the middle letter and 26 choices for each of the other letters. So answer is 5×26^4.

2. Once we choose the first letter, the last letter is determined. So answer is 26^4.

3. $26^4 \times 25$.

4. First choose which year is not represented, then choose the representatives. So answer is $4 \times 5 \times 6 + 4 \times 5 \times 7 + 4 \times 6 \times 7 + 5 \times 6 \times 7 = 638$.

2 More Counting

2.1 Unordered Sets and Binomial Coefficients

In counting sequences, the ordering of the digits or letters mattered. Another common situation is where the order does not matter, for example, if we want to choose a subset of a given size.

> Example 2.1. *Suppose we have* 4 *players, say* A, B, C, D*, but only two can proceed. How many possible pairs are there?*

Well, there are 6 possible pairs: AB, AC, AD, BC, BD, and CD. Note that the order within the pair does not matter: AB is the same as BA.

This is the **binomial coefficient**'s job. The answer we want is abbreviated $\binom{4}{2}$. Some people write this using a capital C, such as ${}_4C_2$, but we will not.

Lemma 2.1 *Given a universe* X *of* n *elements, the number of ways to choose an unordered subset of* X *of* k *elements of without replacement (assuming* $0 \le k \le n$*) is the binomial coefficient*

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

pronounced "n *choose* k*".*

Proof. One way to prove the formula is to argue as follows. Let A be the number of *ordered* sequences of k elements (without replacement) and let B be the number of *unordered* subsets of k elements (without replacement).

We already calculated A in Lemma 1.2 as being $n!/(n-k)!$. But we can also generate all ordered sequences on length k in the following way. Generate all unordered subsets of size k. There are B of these. Then order each of these subsets in all possible ways. We know that a subset of size k can be ordered in $k!$ ways. So this means that:

$$A = B \times k!$$

It follows that $B = n!/(k!(n-k)!)$, as the lemma claims. ◊

This lemma can also be argued in reverse. If we write out all ordered sequences, and group them according to the subset to which they correspond, then each subset will appear $k!$ times. For example, suppose $n = 4$ and $k = 3$. Then there are $4!/(4-3)! = 24$ sequences, but only 4 subsets:

$$\begin{array}{lcl}
\texttt{abc acb bac bca cab cba} & \rightarrow & \{\mathtt{a}, \mathtt{b}, \mathtt{c}\} \\
\texttt{abd adb bad bda dab dba} & \rightarrow & \{\mathtt{a}, \mathtt{b}, \mathtt{d}\} \\
\texttt{acd adc cad adc dac dca} & \rightarrow & \{\mathtt{a}, \mathtt{c}, \mathtt{d}\} \\
\texttt{bcd bdc cbd cdb dbc dcb} & \rightarrow & \{\mathtt{b}, \mathtt{c}, \mathtt{d}\}
\end{array}$$

One obvious property from the symmetry of the formula is that:

Lemma 2.2

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

This fact can also be observed by noting that choosing the k elements in the subset is equivalent to choosing the $n-k$ elements not in the subset.

EXAMPLE 2.2. *Suppose there is a league of 10 teams and every team must play every other team exactly once. How many matches are there?*

The answer is $\binom{10}{2} = 45$.

EXAMPLE 2.3. *How many 5-letter words are there with exactly two vowels?*

Start by choosing the places where the vowels will go. This is 2 places out of 5, so there are $\binom{5}{2} = 10$ ways to do this. Then choose the vowels—5^2—and the consonants—21^3. So the answer is $10 \times 5^2 \times 21^3$.

The above example illustrates a common approach—choose the pattern, then choose the way to fill the pattern.

► **For you to do!** ◄

At the local ice-cream parlor there are 20 mixins, and you get to pick 3 different mixins. Except that 4 of the mixins are "premium" and you cannot have more than one premium mixin. How many possibilities are there? (Hint: there are two choices for the number of premium mixins used.)

2.2 More Examples

Time for some more examples.

EXAMPLE 2.4. *Consider a bag with 4 identical amber balls, 4 identical blue balls, and 4 identical carmine balls. In how many ways can I:*
(a) Pick a subset of the balls?
(b) Pick a subset of 4 balls so that I have at least one ball of each color?
(c) Pick a subset of 7 balls so that I do not have at least one ball of each color?

(a) Because the balls of the same color are identical, it is only the number of each color that matters. There are five possibilities for the number of amber balls (0, 1, 2, 3, 4) and similarly for each of the other colors. So the answer is 5^3.

(b) The only choice we get is which color is doubly represented. Answer is 3.

(c) The subset must have 4 balls of one color and 3 balls of another color. So we get to choose the majority color and then the minority color. The answer is $3 \times 2 = 6$.

EXAMPLE 2.5. *How many anagrams of* `TATTERED` *including nonsense words are there?*

Well, there are 8 letters. But this does not mean there are 8! anagrams, since the order of the `T`'s for example does not matter. (Consider for instance the situation where all the letters are the same!) Note that there are 3 `T`'s and 2 `E`'s, and the remaining letters each appear once. The claim is that the answer is

$$\frac{8!}{3! \times 2!}.$$

One way to see this, is to temporarily add subscripts to the `T`'s and `E`'s. Then list all anagrams: there are indeed 8! if we consider the three `T`'s and two `E`'s as distinct. But if we now erase the subscripts, then a word like `TAREDETT` will appear $3! \times 2! = 12$ times on our list—there are 3! ways of arranging the subscripts on the `T`'s and 2! ways of arranging the subscripts on the `E`'s. So our 8! anagrams can be arranged into groups of 12 identical words. That is, there are $8!/12 = 3360$ anagrams.

Lemma 2.3 *If we have letters $L_1, L_2, \ldots, L_k$ with counts $c_1, c_2, \ldots, c_k$, then the number of anagrams of all the $T = c_1 + c_2 + \ldots + c_k$ letters combined is*

$$\frac{T!}{c_1! \times c_2! \times \cdots \times c_k!}$$

The proof is a repetition of the argument in the above example.

The following example talks about the odds of an event. The **odds** or **chance** of an event is the likelihood of it occurring, or the proportion of time that it occurs. This is calculated by dividing the number of outcomes corresponding to the event in question by the total number of outcomes. (This assumes all outcomes are equally likely; for example, it assumes that the pack of cards is perfectly shuffled.)

EXAMPLE 2.6. *In poker, what are the odds of being dealt a "flush" (all cards are the same suit) ? Let's assume we have a standard 52-card deck, nothing wild, and are dealt* 5 *cards.*

Well there are $\binom{52}{5}$ possible hands. A calculator shows this is 2598960. There are 4 possibilities for the suit. For a fixed suit, there are $\binom{13}{5}$ ways to deal a flush with that suit. Thus the total number of flushes is $4 \times \binom{13}{5} = 5148$. The proportion/chance is 0.198%, or about 1 time in 505.

▶ **For you to do!** ◀

1. To buy a ticket in the local PowwowBall lottery you choose 6 *numbers from the range* 1 *to* 54 *as well as a single Powwow ball in the range* 1 *to* 42*. How many different tickets are there?*

2.3 Multisets

Binomial coefficients turn up in maybe unexpected places.

A **multiset** is like a set except elements can be repeated. One might view it as an "unordered subset with repetition allowed".

EXAMPLE 2.7. *Determine the number of* 3*-element multisets of* $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$.

There are 10 multisets: `aaa`, `bbb`, `ccc`, `aab`, `aac`, `bba`, `bbc`, `cca`, `ccb`, `abc`.

EXAMPLE 2.8. *Determine the number of* 3*-element multisets of an* n*-element set.*

There are three patterns. all three elements the same: n choices;
two of one and one of another: $n \times (n-1)$; and
all three different: $\binom{n}{3}$.
By arithmetic, this sums to $\binom{n+2}{3}$. (Check this yourself!)

The fact that the above example gives a binomial coefficient is no coincidence.

Lemma 2.4 *Given a universe of n elements, the number of ways to choose an unordered multiset of k elements (assuming $0 \leq k$) is*

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

We will prove this in a moment. (And I agree in advance that the proof is intimidating—so you might want to skip it.) But here is an application

> Example 2.9. *Suppose we roll two dice. If the dice are indistinguishable, how many outcomes are there?*

We already calculated this in Example 1.6. Counting dice throws with indistinguishable dice is equivalent to counting unordered multisets. That example corresponds to $n = 6$ and $k = 2$ in the above lemma. The lemma says that the number of outcomes is $\binom{7}{2} = 21$, which is what we determined originally.

Okay, here is the proof of the lemma.

Proof of Lemma 2.4. We will count something that is the same size.

Fix some ordering of the n-element universe X. The key idea is that each k-element multiset S from X can be represented by a sequence of $k + n - 1$ white and black circles of which k are white, and vice versa.

The recipe is to write S on a line. Then insert a black circle for every for every change in X. Then convert every element of S to a white circle.

For example, suppose $X = \{\texttt{a}, \texttt{b}, \texttt{c}, \texttt{d}, \texttt{e}, \texttt{f}\}$ and consider `aacd`. Then we have

a a c d

a a ● ● c ● d ● ●

○ ○ ● ● ○ ● ○ ● ●

Now, the claim is that this process is reversible; That is, we can get from the circles to the multisets. We start with `a` and every time we hit a dark circle we increment it. Furthermore, and this is the magical thing, every possible sequence of circles with $k - 1$ blacks corresponds to a multiset.

And so, counting the number of multisets is the same as counting the number of circle sequences. And there are $\binom{n+k-1}{k}$ of those. $\Diamond$

> EXAMPLE 2.10. *Suppose we have* 7 *numbered boxes in a row. We have* 10 *indistinguishable balls. In how many ways can we place the balls into the boxes?*

If we write down the labels of the boxes taken, this problem is equivalent to choosing a 10-element multiset from a 7-element universe. By the above lemma, this is the binomial coefficient $\binom{16}{10}$.

The lemma explains the answer to the question of unordered subsets with repetition allowed.

Exercises

2.1. A contest has 5 prizes: TV, ipod, cellphone, bicycle, vacation. You get to pick 2 of them, except that you cannot pick two electronic goods. How many possibilities do you have?

2.2. Calculate $\binom{2}{1}$, $\binom{4}{2}$, $\binom{6}{3}$, $\binom{8}{4}$, and $\binom{10}{5}$.

2.3. An SSN is a 9-digit number with zeroes allowed in every position.

(a) How many SSNs have exactly two distinct digits?

(b) How many SSNs have digits that sum to 2?

(c) How many SSNs have digits that sum to 3?

2.4. How many 5-letter words are there with exactly 4 different letters?

2.5. Determine the number of anagrams of:

(a) `SASSAFRAS`

(b) `BOOKKEEPER`

2.6. A pizza place offers 5 different meat toppings, and 10 different vegetable toppings. (In each of the following the order of the toppings does not matter.)

(a) A *meat-and-three* pizza has 1 meat and 3 different vegetable toppings. How many meat-and-three pizzas are there?

(b) A *double-play* has only 2 toppings, but these can be the same topping. How many double-play pizzas are there?

(c) A *glutton* pizza has 6 different toppings of which at most 4 can be meat. How many glutton pizzas are there?

2.7. I have a bag containing 12 numbered balls of which 4 are red, 4 are green, and 4 are blue. In how many ways can I choose an unordered set of:

(a) 7 balls?

(b) 6 balls if I must have equal numbers of each color?

(c) 4 balls if I must have at least one of each color?

(d) 4 balls if I must have more red than green?

2.8. Let us define a **key** as a 6-digit number with zeroes allowed in every position, such as `043771`.

(a) How many possible keys are there with all digits distinct?

(b) How many possible keys are there if the digits sum to 3?

(c) How many possible keys are there if the key contains exactly two distinct digits?

2.9. Consider three balls and three buckets. In how many different ways can the balls be arranged in the buckets if:

(a) the balls and the buckets are all numbered?

(b) the balls are numbered but the buckets are indistinguishable?

(c) the buckets are numbered but the balls are indistinguishable?

(d) the balls are indistinguishable and the buckets are indistinguishable?

2.10. Wayne has a pile of 20 books to read.

(a) In how many orderings can he read them?

(b) In how many orderings can he read them if the pile includes the 7 Harry Potter books, which must be read in order and consecutively?

(c) How many orderings if the 7 Harry Potter books must be read in order but not necessarily consecutively?

2.11. Suppose I have a bag with X balls labeled 1 up to X, with X even. Half the balls are orange and half the balls are purple.

(a) In how many ways can I choose a subset of 3 balls such that their labels sum to at most 8? (Assume X is large.)

(b) In how many ways can I choose a subset of 4 balls such that I get at least one ball of each color.

2.12. Jabber is played with a 30-card deck: there are three suits and the cards are numbered 1 up to 10. A player receives 4 cards.

(a) How many possible jabber hands are there?

(b) A straight contains cards of consecutive values, such as 5, 6, 7 8, but they can be of different suits. How many possible straights are there?

(c) A flush has all cards the same suit. How many possible flushes are there?

(d) A straight flush is a hand that is both a straight and a flush. How many possible straight flushes are there?

2.13. In the local lottery, you buy a ticket with 6 (unordered) numbers in the range 1 to 49, and you have to match the 6 numbers drawn to win the jackpot.

(a) Calculate $\binom{49}{6}$.

(b) A runner-up prize is obtained if you match exactly 5 of the drawn numbers. Calculate the odds of a runner-up prize.

(c) All tickets that match no numbers are placed in a barrel for a chance at a "lucky loser" prize. Calculate the odds of a particular ticket matching no numbers.

2.14. Consider a 5-card poker hand.

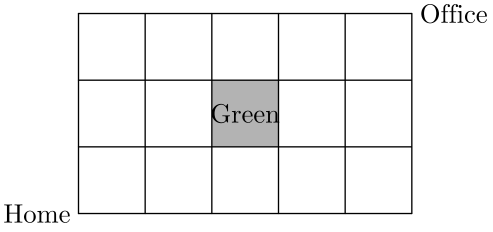
(a) Calculate the odds of being dealt a "full house" (3 of one denomination/rank and 2 of another).

(b) Calculate the odds of being dealt a "royal flush" (ace, king, queen, jack, and ten of the same suit).

(c) Calculate the odds of being dealt "two pairs" (2 of one denomination, 2 of another denomination, and the remaining card a third denomination).

2.15. Consider 3-digit numbers, no zeroes allowed. How many such numbers are there with the digits strictly increasing?

2.16. Mabe lives in Manhattan and his office is 5 blocks east and 3 blocks north. He always takes the shortest route to work (that is, he walks exactly 8 blocks), but he likes to vary the route.



(a) How many different shortest routes can Mabe take between his home and his office?

(b) How many different shortest routes can Mabe take if he wants to walk along two sides of the central green?

(c) How many different shortest routes can Mabe take if he wants to avoid the central green completely (even at its corners)?

2.17. How many different necklaces can be made with 7 beads: 3 red, 2 blue, and 2 white? Note that a necklace has no starting point, and that flipping it over gives the same necklace.

2.18. Suppose we have 12 people and need to split them into three subcommittees of size 3, 4 and 5, with nobody serving on more than one subcommittee. In how many ways can this be done?

2.19. On Planet X all the people are of the same gender. Nevertheless, they still pair off each year to get married in one simultaneous ceremony. There are 10 people on planet X. How many possible marriage ceremonies are there?

Solutions to Practice Exercises

1. You get either three non-premiums or two non-premiums and one premium. Thus the answer is $\binom{16}{3} + \binom{16}{2}\binom{4}{1}$.

2. Answer is $42 \times \binom{54}{6}$.

3 Properties of Binomial Coefficients

3.1 Properties of Binomial Coefficients

Here is the famous recursive formula for binomial coefficients.

Lemma 3.1 *For $1 \le k < n$,*

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

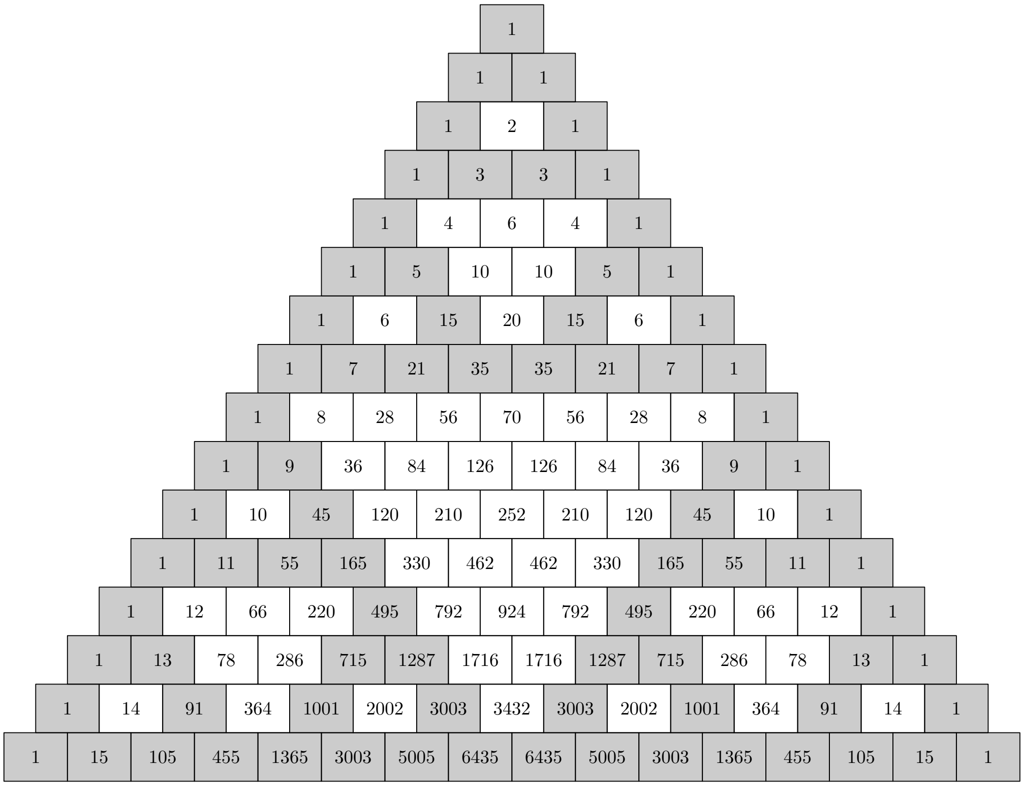
This equation can be proven by replacing each binomial coefficient by its ratio of factorials and checking that we get the same on both sides. (Do it!)

However, mathematicians like proofs that explain *why* something is true: a **combinatorial proof** of an equation is where both sides are shown to count the same thing.

Proof. In the above equation, the LHS (left-hand side) by definition counts the unordered subsets of size k. Now, let a be the first element of the universe. A subset either contains a or it doesn't. If the subset contains a, then what remains is a subset of size $k-1$ from the remaining universe of size $n-1$. If the subset does not contain a, then it is a subset of size k from the remaining universe of size $n-1$. So by the sum rule, the RHS (right-hand side) also counts the unordered subsets of size k: the first binomial coefficient counts those with a and the second binomial coefficient counts those without. $\diamondsuit$

Binomial coefficients can be arranged in what is called **Pascal's triangle** (even though multiple cultures investigated it long before Pascal). Pascal's triangle has the rule that each entry is the sum of the two entries immediately above it, and so the n^{th} row from the top is the binomial coefficients $\binom{n}{k}$. Many thousands of pages have been written about the properties of binomial coefficients and their kin.

For example, the remainders when binomial coefficients are divided by a prime provide interesting patterns. Here is the start of Pascal's triangle with the odd binomial coefficients shaded.



1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 28 56 70 56 28 8 1

1 9 36 84 126 126 84 36 9 1

1 10 45 120 210 252 210 120 45 10 1

1 11 55 165 330 462 462 330 165 55 11 1

1 12 66 220 495 792 924 792 495 220 66 12 1

1 13 78 286 715 1287 1716 1716 1287 715 286 78 13 1

1 14 91 364 1001 2002 3003 3432 3003 2002 1001 364 91 14 1

1 15 105 455 1365 3003 5005 6435 6435 5005 3003 1365 455 105 15 1

Here is another famous fact about binomial coefficients.

Theorem 3.2 *For $n \geq 0$,*

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

Proof. We give a combinatorial proof. Let X be an n-element set, and let Y be the set of subsets of X. In Example 1.4 we observed that $|Y| = 2^n$.

On the other hand, let us count Y by considering the sizes of each subset. Then, by Lemma 2.1 there are $\binom{n}{k}$ of size k, and so, if we sum this quantity from $k = 0$ to $k = n$, we get $|Y|$. Thus the two sides of the above equation are in fact equal. $\Diamond$

If we use what is called sigma-notation, then the above equation can be rewritten as

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

In the expression $\sum_{k=0}^{n}$, it means to loop through all values from $k = 0$ to $k = n$, evaluate the formula, and add up all the results.

The result in the previous theorem is generalized in the famous **Binomial Theorem**. (It's a generalization, because if we plug $x = y = 1$ into the Binomial Theorem, we get the previous result.)

Theorem 3.3 (Binomial Theorem)

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

Proof. Let's start by showing the idea in a specific case. Consider $n = 3$. Then the LHS product is $(x+y)(x+y)(x+y)$. If we multiply this out, but do not use the commutative law for multiplication, we get $xxx+xxy+xyx+xyy+yxx+yxy+yyx+yyy$. Now, to get the coefficient of x^2y say, we group together xxy, xyx, and yxx. That is, the coefficient of x^2y is the number of ways of creating a "word" using exactly x, x, and y. To count such, we choose the positions for the y's: this is a subset of size k.

The real proof is exactly the above idea but with notation. The total number of $x^{n-k}y^k$ in $(x+y)^n$ is equal to the number of ways of placing the k y's in a word together with $n-k$ x's; this is the binomial coefficient $\binom{n}{k}$. ♢

Example 3.1. *What is the coefficient of x^2y^5 if we multiply out $(x+y)^7$?*

By the Binomial Theorem, it is $\binom{7}{5}$ (or $\binom{7}{2}$ if you prefer).

▶ **For you to do!** ◀

1. Take several deep breaths.

Exercises

3.1. Provide a combinatorial proof of the identity:

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

(Hint: Consider a three-person subcommittee with a leader.)

3.2. (a) Show that

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

provided k is positive.

(b) Give a combinatorial proof of this.

3.3. Consider the equation

$$\binom{n}{200}\binom{200}{20} = \binom{n}{20}\binom{n-20}{180}$$

(a) Use algebra and the formula for binomial coefficients to prove this equation.

(b) Provide a combinatorial proof of this equation. (Hint: consider choosing a committee and a subcommittee.)

3.4. Show that if p is a prime number, then $\binom{p}{i}$ is a multiple of p for all i from 1 up to $p-1$.

3.5. Consider the following identity:

$$\sum_{0 \le i \le n/2} \binom{n}{2i} = \sum_{0 \le i < n/2} \binom{n}{2i+1}.$$

For example, when $n = 3$ it claims that $\binom{3}{0} + \binom{3}{2} = \binom{3}{1} + \binom{3}{3}$; this is true since both sides equal 4.

(a) Verify this identity for $n = 4$ and $n = 5$.

(b) Deduce this identity from the Binomial Theorem (by plugging in suitable value of x and y).

(c) Give a combinatorial proof of the identity.

3.6. Consider the following identity:

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

For example, when $n = 2$ it claims that $\binom{2}{0}^2 + \binom{2}{1}^2 + \binom{2}{2}^2 = \binom{4}{2}$; this is true since both sides equal 6.

(a) Verify this identity for $n = 3$ and $n = 4$.

(b) Give a combinatorial proof of the identity. (Hint: consider a $2n$-element set with half its elements colored red.)

3.7. Just like $\sum$ for addition, there is $\prod$ for multiplication. Show that

$$\binom{n}{k} = \prod_{i=1}^{k} \frac{n-k+i}{i}$$

3.8. (a) Using some mathematics software or a calculator, calculate $\binom{50}{25}$.

(b) In Java (and usually in C) an `int` variable has a maximum value of 2^{31}. Explain why we cannot use `int`'s to calculate 50!.

(c) Write code using the recursive formula from Lemma 3.1 to calculate $\binom{50}{25}$. (Note that you will need to stop the recursion under certain circumstances.)

(d) Write code using the formula from Exercise 3.7 to calculate $\binom{50}{25}$.

(e) Comment on the efficiency of your code.

3.9. Prove that $\binom{2000}{1000}$ is even.

3.10. Suggest and prove a generalization of the Binomial Theorem of the form $(x+y+z)^n = \sum \ldots$.

4 Relations and Functions

In this section we consider (and count) mathematical objects called functions, partitions, relations, and equivalence relations.

4.1 Functions

You have seen functions before. A **function** has a **domain** and a **codomain**. The function maps each element in the domain to an element in the codomain; that is, given any element of the domain, the function evaluates to a specific value in the codomain. The **range** of a function is the set of elements in the codomain which really do have something mapping to them.

Example 4.1.

Suppose that $f(x) = x^2 - 4$ with domain and codomain all real numbers. Then the range is all real numbers at least -4. This is equivalent to asking for which y does there exist an x such that $y = x^2 - 4$.

Note that the domain must be given as part of the definition of the function; so should the codomain.

There are three special types of function:

- A function is said to be **one-to-one** if every element in the range is mapped to by a unique element in the domain.
- A function is said to be **onto** if every element in the codomain is mapped to; that is, the codomain and the range are equal.
- A function is said to be a **bijection** if it is both one-to-one and onto.

In the above example, the function f is not one-to-one; for example, $f(3) = f(-3)$. The function is also not onto; for example, there is no x such that $f(x) = -7$. The key point about a one-to-one function is that it is reversible, in that if you tell me $f(x)$ I can work out x.

Example 4.2. *For each of the following functions, the domain and the codomain are the set of all integers. Determine which of the functions are one-to-one and*

which are onto.
(a) $f(x) = x + 1$
(b) $f(x) = 2x$
(c) $f(x) = x/2$ *if* x *is even and* $(x + 1)/2$ *if* x *is odd.*

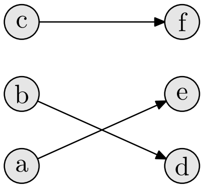
(a) This is a bijection.

(b) This is one-to-one but not onto. (The range is all even integers.)

(c) This is onto but not one-to-one. (For example, $f(1) = f(2)$.)

Some people (including me) like to represent a function using a collection of arrows. The domain is on the left and the codomain on the right and there is exactly one arrow leading out of each element on the left.

EXAMPLE 4.3. *Here is a depiction of a bijection from* $\{a, b, c\}$ *to* $\{d, e, f\}$.



We observe the following elementary properties of functions, whose proof we leave as an exercise. (Actually, this lemma requires a bit of thought—for example, I got range and codomain mixed up the first time I wrote it down. . . sigh.)

Lemma 4.1 *Let* f *be a function with a finite domain and codomain.*
(a) The range is at most the size of the domain.
(b) If f *is one-to-one, then the codomain is at least as large as the domain.*
(c) If f *is onto, then the codomain is at most as large as the domain.*
(d) If f *is a bijection, then the domain and range are the same size.*
(e) If the domain and range are the same size, then f *is onto if and only if it one-to-one if and only if it is a bijection.*

EXAMPLE 4.4. *Let* $A = B = \{0, 1\}$.
(a) How many functions are there from A *to* B*?*
(b) How many onto functions are there from A *to* B*?*
(c) How many one-to-one functions are there from A *to* B*?*
(d) How many bijections are there from A *to* B*?*

(a) To specify each function, we must specify where each member of A gets mapped to. That is, we choose what 0 gets mapped to and what 1 gets mapped to. We have two choices for each, so the answer is $2^2 = 4$.

(b,c,d) By Lemma 4.1e, the answers to these three parts are the same. A bijection means we pair off elements of A with elements of B. There are only two possibilities: the function that maps $0 \to 0$ and $1 \to 1$, and the function that maps $0 \to 1$ and $1 \to 0$.

► For you to do! ◄
Let $S = \{a, b, c, d, e\}$.
1. How many functions from S to S are there?
2. How many one-to-one *functions from S to S are there?*

4.2 Partitions

A **partition** of a set is writing it as the disjoint union of nonempty **blocks**. (Recall that disjoint means non-overlapping.) For example, $\{\{1\}, \{3, 5\}, \{2, 4\}\}$ is a partition of the set $X = \{1, 2, 3, 4, 5\}$. Note that the order of the blocks does not matter, and neither does the order of the elements within a block.

Example 4.5. *Determine all partitions of the set $\{a, b, c\}$.*

There are 5 partitions. There is 1 partition into one block. There is 1 partition into three blocks (where every element is in a block by themselves). There are 3 partitions into two blocks: based on which of the elements is in a block by itself. We might write these partitions as:

abc
$a \mid bc$ $b \mid ac$ $c \mid ab$
$a \mid b \mid c$

4.3 Relations

In English we often say something is "related to" or "similar to" or "connected to" something else. This could be because they share genes, or one thing causes the other thing, or because they are different colors. Mathematics tries to capture this notion with what it calls a "relation". To specify a relation, we can give a rule which explains when two things are related, for example, when they are different colors. More generally, we can specify a function by listing all the pairs of related elements. Examples of relations include “same color as”, “is a subset of”, and “is a neighbor of”.

Mathematically, a **relation** on a universe X is a set of ordered pairs on X. If R stands for the relation, then we will write xRy to mean that x is related to y in the relation R. For example, if R was the “equality relation”, we would write that $x = y$. Though we will do it in the following example, it is usually impossible to write out all the ordered pairs, since there are often infinitely many of them.

> EXAMPLE 4.6. *Assume the universe is* $X = \{0, 1, 2, 3\}$. *What is the usual name for the following relations?*
> *(a)* $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$
> *(b)* $\{(0, 1), (1, 2), (2, 3), (0, 2), (1, 3), (0, 3)\}$
> *(c)* $\{(0, 0), (1, 1), (2, 2), (3, 3), (1, 3), (0, 2), (2, 0), (3, 1)\}$

(a) Equal to
(b) Less than
(c) Has the same parity as (same remainder when divided by 2).

4.4 Equivalence Relations

We are interested in relations that have three specific properties:

- A relation R is **reflexive** if xRx for all x (that is, everything is defined to be related to itself).
- A relation R is **symmetric** if xRy always implies yRx; and
- A relation is **transitive** if xRy and yRz being true always implies xRz.

For example, the relation “less than” is transitive: if $a < b$ and $b < c$ then it necessarily follows that $a < c$. And, the relation “is a neighbor of” is symmetric: if I’m your neighbor then necessarily you’re my neighbor.

An **equivalence relation** is one that is reflexive, symmetric, and transitive.

> EXAMPLE 4.7. *Consider all the people in the world. We can define two people to be related if they have the same name. Show that this relation, call it* S, *is an equivalence relation.*

There are three properties to check. I have the same name as myself; so S has the reflexive property. If I have the same name as you, then you have the same name as me; so S has the symmetric property. If person X has the same name as person Y and person Y has the same name as person Z, then certainly persons X and Z have the same name; so S has the transitive property. That is, the three properties of an equivalence relation are satisfied.

In an equivalence relation, the **equivalence class** of element x is the set of all elements related to it (note that x is in its own equivalence class, by the reflexive property). That is, an equivalence class is a set of elements that are considered to be similar or equivalent.

> EXAMPLE 4.8. *Let $\mathbb{N}$ be the set of all nonnegative integers. Define the relation M so that xMy if and only if x and y have the same units digit. Show that M is an equivalence relation and determine the equivalence classes.*

This is an equivalence relation. For example, to check that it is transitive, we note that if x and y end in the same digit, and y and z end in the same digit, then it must be the case that x and z end in the same digit.

There are 10 equivalence classes—one for all numbers ending with a `0`, one for all numbers ending with a `1`, and so on.

Theorem 4.2 *For any equivalence relation R, any two equivalence classes are either disjoint or equal.*

PROOF. Let R denote the equivalence relation, and let E_x and E_y denote the equivalence class containing x and y respectively. Assume that E_x and E_y are not disjoint. Then that means there is some common element, call it z.

Now, let a be some element of E_x. By definition, this means that aRx. Further, we have that xRz (since z is in E_x) and that zRy (since z is in E_y). So it follows that aRy (by the transitive property). That is, $a \in E_y$. And the converse holds: if $b \in E_y$, then $b \in E_x$.

That is, we have shown that every element of E_x is also an element of E_y and vice versa. This means that $E_x = E_y$. $\Diamond$

The theorem means that if you tell me the equivalence classes, I can work out the equivalence relation. In particular, the theorem means that the equivalence classes form a partition of X. But the connection goes the other way too: every partition gives rise to an equivalence relation. (Think about why...)

Lemma 4.3 *If X is some universe, there is a bijection between the set of equivalence relations on X and the set of partitions of X.*

Equivalence relations are useful in counting. Indeed, we already implicitly did this, when we said two things were to be considered the same even though we counted them twice. Recall that we proved that the number of k-element subsets of an n-element set is $\binom{n}{k}$, by counting k-element sequences and arguing that each k-element subset arose from $k!$ such sequences.

In general, if we count some set X by counting some process that generates elements of X, then we have to divide by the number of ways each element of X is produced. This can stated as the Quotient Principle:

Lemma 4.4 *If we partition a universe of size p into q blocks of size r, then $q = p/r$.*

> **► For you to do! ◄**
> *Let $\mathbb{Z}$ be the set of all integers (positive and negative). In each case, determine whether the relation on $\mathbb{Z}$ is an equivalence relation or not, and justify your answer.*
> *3. N is the "nothing" relation. That is, no element is related to any other element, not even itself.*
> *4. A is the "absolute value" relation. That is, two elements are related if their absolute value is the same.*
> *5. B is the "bigger than". That is, xBy if and only if $x > y$.*

Exercises

4.1. Suppose $|A| = |B| = 100$. How many functions are there from A to B? How many of these functions are bijections?

4.2. Convince your grandmother that Lemma 4.1 is true.

4.3. Consider the function $f(x) = x^2$.

(a) Give an example of domain and codomain such that the function f is onto but not 1–1.

(b) Give an example of domain and codomain such that the function f is 1–1 but not onto.

(c) Give an example of domain and codomain such that the function f is a bijection.

4.4. Let $A = \{a, b\}$ and $B = \{c, d, e\}$.

(a) How many functions are there from A to B?

(b) How many onto functions are there from A to B?

(c) How many one-to-one functions are there from A to B?

(d) How many bijections are there from A to B?

4.5. Let $Y = \{t, u, v, w\}$ and $Z = \{x, y, z\}$.

(a) How many functions are there from Y to Z?

(b) How many onto functions are there from Y to Z?

(c) How many one-to-one functions are there from Y to Z?

(d) How many bijections are there from Y to Z?

4.6. List all partitions of the set $\{a, b, c, d\}$. (Hint: there are 15.)

4.7. How many partitions are there of a 5-element set?

4.8. In how many ways can an 100-element set be partitioned into

(a) 101 blocks?

(b) 100 blocks?

(c) 99 blocks?

(d) 98 blocks?

4.9. Let $S(n, k)$ denote the number of partitions of an n-element set into a partition with k blocks.

(a) Explain why $S(n, 1) = 1$, $S(n, n) = 1$, and $S(n, k) = 0$ if $k > n$.

(b) Explain why $S(n, k) = S(n - 1, k - 1) + kS(n - 1, k)$.

(c) Use this to calculate the number of partitions of a 6-element set.

4.10. Consider the set $S = \{a, b, c, d, e\}$ and the partition $P = \{\{a\}.\{b, c\}, \{d, e\}\}$. Write down the ordered pairs of the equivalence relation on S whose equivalence classes are given by P.

4.11. Let $<$ be the "less-than" relation with universe the positive integers;

let D be the relation with universe all sets, such that two sets are related if they are disjoint

let $\approx$ be the relation with universe all real numbers, such that x and y are related if $|x - y| < 0.01$.

Complete the following table (with "yes" and "no"):

	$<$	D	$\approx$
Reflexive			
Symmetric			
Transitive			

4.12. Let the universe be $\mathbb{N}$ the set of all nonnegative integers. In each of the following, determine whether the relation is an equivalence relation. If it is not, state one property it fails to have; if it is, state the number of equivalence classes.

(a) E is the "everything" relation. That is, every number is related to every number.

(b) N is the "nothing" relation. That is, no number is related to any other number, not even itself.

(c) P is the "parity" relation. That is, two numbers are related if they are both even, or if they are both odd.

(d) L is the "less than or equal" relation. That is, x is related to y if $x \leq y$.

4.13. Let the universe be all 178,691 words in the official English Scrabble dictionary. In each of the following, determine whether the relation is an **equivalence relation**. If it is not, state one property that the relation fails to have. If it is, state the number of equivalence classes.

(a) S is the "start" relation. That is, words x and y are related if they have the same initial letter.

(b) L is the "loner" relation. That is, every word is related to itself but not to any other other word.

(c) N is the "nothing" relation. That is, no word is related to any word, not even themselves.

(d) A is the "alphabetical" relation. That is, xAy if x occurs before y in the dictionary.

(e) O is the "one-letter" relation. That is, xOy if x and y differ by exactly one letter.

4.14. Give an example of a symmetric relation that is:

(a) Reflexive and transitive

(b) Reflexive and not transitive

(c) Transitive and not reflexive

4.15. Let A be the set of all positive integers and let $X = A \times A$. Define a relation R on X by saying that $(a, b)\,R\,(c, d)$ iff $ad = bc$. Show that R is an equivalence relation. Would R still be an equivalence relation if A was the set of all integers?

4.16. Let X be the set of all words in the English dictionary. In each case, determine whether the relation on X is an equivalence relation or not. If it is an equivalence relation, determine how many equivalence classes there are. If it is not an equivalence relation, state one of the three conditions the relation does not obey.

(a) G is the "geography" relation. That is, xGy if word y begins with the same letter that word x ends with (for example, CAT is related to TIGER but not vice versa).

(b) F is the "first-letter" relation. That is, xFy if words x and y begin with the same letter.

(c) P is the "contains-`p`" relation. That is, two words are related if either they both contain a `p`, or if neither contains a `p`.

4.17. Some books define a function as a special type of relation. Suggest how such a definition might go.

Solutions to Practice Exercises

1. 5^5 (five choices for each element of the domain).

2. 5! (five choices for $f(a)$, four choices for $f(b)$, and so on.)

3. Not an equivalence relation. For example, not reflexive.

4. Is an equivalence relation.

5. Not an equivalence relation. For example, not symmetric.

5 Logic

In this part of the course we consider logic. Logic is used in many places in computer science including digital circuit design, relational databases, automata theory and computability, and artificial intelligence.

We start with propositional logic, using symbols to stand for things that can be either true or false. Then we consider the concept of proof in mathematics. Finally we consider some more concepts from symbolic logic.

5.1 Statements

A **statement** *is a sentence that is definitely either true or false but not both.*

For example: "*Two plus two equals four.*" and "*Two plus two equals five.*" are both statements. The sentence "*He is a college student.*" is not a statement, since information is missing and it could be either true or false.

A **compound statement** *is a combination of statements using the words* ***not, and,*** *and* ***or****.*

5.2 Operators and Truth Tables

We represent statements by **boolean variables** and form compound statements using **logical connectives** or **operators**. The three standard operators are **not**, **and**, and **or**.

If p and q are (compound) statements,
the **negation** *of p is* ***not*** *p, denoted $\neg p$;*
the **conjunction** *of p and q is p* ***and*** *q, denoted $p \wedge q$;*
the **disjunction** *of p and q is p* ***or*** *q, denoted $p \vee q$, which is true when at least one of p and q are true; and*
the **exclusive or** *of p and q is denoted $p \oplus q$, which is true when exactly one of p and q is true.*

Note that English is inherently sloppy when using the "or". So we introduced two operators: the "**(inclusive) or**", where the two parts can happen simultaneously, and the "**exclusive or**", where the two parts cannot happen simultaneously.

> *A* **truth table** *gives the truth value of a compound statement for every combination of truth values of its variables.*

Here are the truth tables for the three binary operators defined above.

s	t	$s \wedge t$	$s \vee t$	$s \oplus t$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

Example 5.1. *Here is the truth table for* $\neg p \wedge \neg q$.

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
F	F	T	T	T
F	T	T	F	F
T	F	F	T	F
T	T	F	F	F

5.3 Logical Equivalence

> *Two compound statements are* **logically equivalent** *if they have the same truth value for every setting of their variables. The symbol for logical equivalence is* $\equiv$.

The standard/initial method for proving logical equivalence is to construct a truth table for both sides.

Example 5.2. *Show that the associative rule holds for conjunction; that is,* $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
F	F	F	F	F	F	F
F	F	T	F	F	F	F
F	T	F	F	F	F	F
F	T	T	F	F	T	F
T	F	F	F	F	F	F
T	F	T	F	F	F	F
T	T	F	T	F	F	F
T	T	T	T	T	T	T

Since the two columns corresponding to the two statements are identical, we have shown that they are logically equivalent.

Example 5.3. *One can show that:*

$$\neg p \wedge \neg q \equiv \neg (p \vee q)$$

This is called **de Morgan's law**. *There is another version where the $\wedge$'s and the $\vee$'s are interchanged:*

$$\neg p \vee \neg q \equiv \neg (p \wedge q)$$

A **tautology** *is a (compound) statement that is always true. A* **contradiction** *is a (compound) statement that is always false.*

For example, $p \vee \neg p$ is a tautology.

5.4 Conditionals and Biconditionals

When we make a logical deduction, we reason from a **hypothesis** to a **conclusion**. The aim is to be able to say: "***If*** *such and such is known,* ***then*** *something or other must be the case".*

A ***conditional statement*** *or* **implication** *is a statement of the form "If p then q", denoted $p \Rightarrow q$.*

The truth table for implication is:

p	q	$p \Rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

This is sometimes translated as "p is sufficient for q", or "$\neg p$ is necessary for $\neg q$".

It is useful to remember that:

- $p \Rightarrow q \equiv \neg p \vee q$
- The **converse** of $p \Rightarrow q$ is $q \Rightarrow p$.

- The **contrapositive** of $p \Rightarrow q$ is $\neg\, q \Rightarrow \neg\, p$. The contrapositive is logically equivalent to the original.

A ***biconditional statement*** *is a statement of the form "p if and only if q", denoted* $p \Leftrightarrow q$.

The truth table for this is:

p	q	$p \Leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

This is sometimes translated as "p is necessary and sufficient for q".

Note that there is precedence: we assume the "not" applies to the smallest piece it can; and that the arrows apply to the largest piece they can. For example, $p \vee \neg\, q \Rightarrow r \wedge s$ should be read as $(p \vee (\neg\, q)) \Rightarrow (r \wedge s)$. It is common to assume that "**and**" has higher precedence than "**or**", such as in the Java and C programming languages. However, we do not assume that here, using parentheses instead.

Exercises

5.1. Construct a truth table for the following compound statement:

$$(p \vee (\neg\, p \vee q)) \wedge \neg\, (q \wedge \neg\, r)$$

5.2. Use truth tables to determine which of the following pairs of statements are logically equivalent.

(a) $p \vee (p \wedge q)$ versus p

(b) $\neg\, (p \vee q)$ versus $\neg\, p \wedge \neg\, q$

(c) $(p \vee q) \vee r$ versus $p \vee (q \vee r)$

(d) $(p \wedge q) \vee r$ versus $p \wedge (q \vee r)$

(e) $((\neg\, p \vee q) \wedge (p \vee \neg\, r)) \wedge (\neg\, p \vee \neg\, q)$ versus $\neg\, (p \vee r)$

5.3. Assuming s is a statement, simplify the following:

(a) $s \wedge \mathsf{T}$

(b) $s \vee \mathsf{T}$

(c) $s \wedge \mathsf{F}$

(d) $s \vee \mathsf{F}$

(e) $s \Rightarrow \mathsf{T}$

(f) $s \oplus \mathsf{F}$

5.4. Use De Morgan's law to write the negation of the compound statement:

$$1 < x \leq 3$$

5.5. Establish which of the following are tautologies and which are contradictions.

(a) $(p \wedge q) \vee (\neg p \vee (p \wedge \neg q))$

(b) $(p \wedge \neg q) \wedge (\neg p \vee q)$

5.6. For the statement "If a tiger roars, then a cock cowers", state:

(a) the converse

(b) the contrapositive

5.7. Give the converse, contrapositive, and negation of: "If Sue is Luiz's mother then Deana is his cousin."

5.8. Construct truth tables for the following:

(a) $(p \Rightarrow q) \Rightarrow (q \Rightarrow p)$

(b) $(p \oplus q) \Rightarrow (\neg r \Leftrightarrow (p \vee q))$

5.9. Suppose we have a situation where there are n boolean variables and we want a boolean function where we specify individually the truth value for every setting of the variables. Show that it is always possible to construct such a compound statement using only $\wedge$, $\vee$, and $\neg$ as operators. Estimate the size of your statement.

5.10. We showed in the previous question that every compound statement has an equivalent statement that uses only $\wedge$, $\vee$, and $\neg$.

(a) Prove that every compound statement has an equivalent statement that uses only $\wedge$ and $\neg$ as operators.

(b) The NAND connective is defined by the following table:

s	t	s NAND t
T	T	F
T	F	T
F	T	T
F	F	T

Show that every compound statement has an equivalent statement that uses only NAND as an operator.

6 Proofs

6.1 Direct Proof

In an ideal world, a **direct proof** is a "sequence of statements each of which is a hypothesis, a fact, or inferred from previous statements using valid rules of inference."

Consider for example, a standard introductory exercise: "Prove that the square of an even integer is even." First, note that math-speak often omits an implied "every". What this exercise is really saying is: "Prove that the square of every even integer is even." Second, note that the task can be recast as a conditional statement: "Prove that if you have an even integer then its square is even". To prove a conditional, one assumes the hypothesis and attempts to infer the conclusion.

We also need the principle of "**universal generalization**": If one can prove statement about x by assuming only that x is a member of osome universe, then one can conclude the statement is true for every member of that universe.

We can now try a proof. But we still need to know the definition of an even integer. For this chapter, we will **define** an integer m as **even** if it is equal to $2i$ for some integer i, and define m as **odd** if it is equal to $2i + 1$ for some integer i.

Example 6.1. *Prove that the square of an even integer is even.*

Let x be an even integer. Then there is an integer i such that $x = 2i$. Thus $x^2 = (2i)^2 = 4i^2 = 2 \times (2i^2)$. Note that $2i^2$ is an integer. It follows that x^2 is two times an integer and is therefore even.

(Of course, it is admittedly artificial that one knows the properties of integers but has to prove the properties of even-ness. . .) Here is a similar example.

Example 6.2. *Prove that the sum of two odd integers is even.*

Let m and n be odd integers. Then there are integers i and j such that $m = 2i + 1$ and $n = 2j + 1$. This means that $m + n = (2i + 1) + (2j + 1) = 2(i + j + 1)$. Thus $m + n$ is two times an integer and is therefore even. Thus by universal generalization, the sum of any two even integers is even.

▶ **For you to do!** ◀

1. Prove that if $x^2 - 1$ is a multiple of 3, then x is not a multiple of 3.

6.2 Disproofs and Counterexamples

To prove a statement such as “all roses are red”, one needs a proof that works for all roses. To prove a statement is false, one needs only one case where it fails: one rose that is not red. This is called a **counterexample**. For example, suppose the claim is that “All primes are odd”. But 2 is prime and even.

Example 6.3. *Prove or disprove: For all real numbers x and y it holds that $|x+y| = |x| + |y|$.*

Well, this statement is false. For a counterexample, let $x = 1$ and $y = -1$.

6.3 Proof by Contradiction

In a proof by contradiction, we **suppose** the negation of what we are trying to prove and try to reach a contradiction. If every step of the proof is valid, then the only possible reason for the contradiction is that the supposition is false.

For example, here is a famous proof by contradiction that $\sqrt{5}$ is not rational. (A number is rational if it can be expressed as the ratio of two integers.)

Example 6.4. *Prove that $\sqrt{5}$ is irrational.*

Suppose $\sqrt{5}$ is rational. Then

$$\sqrt{5} = m/n$$

for some integers m and n. We can simplify the fraction so that m and n do not have a common factor. Now, $5 = m^2/n^2$ and thus $m^2 = 5n^2$. It follows that m^2 is a multiple of 5 and so m is a multiple of 5. That is, $m = 5r$ for some integer r.

Then $m^2 = 25r^2$ and so $n^2 = 5r^2$. By the same reasoning, n is a multiple of 5. Thus, m and n have a common factor (namely 5); this is a contradiction. Thus by the principle of proof by contradiction, $\sqrt{5}$ is not rational.

6.4 Valid Rules of Inference and Fallacies

In the proofs above we used deduction or inference. For example we used already the rule of inference called modus ponens:

Modus ponens. *The rule of inference: “From p and $p \Rightarrow q$, we may deduce q”*

For example, assume we know that "all roses are red" and that "Pete is a rose". It follows by modus ponens that "Pete is red".

But how do we know that this rule is valid? Well, we can *prove* it.

A rule of inference consisting of statements $s_1, s_2, \ldots, s_n$ and assertion q is **valid** *if $s_1 \wedge s_2 \wedge \ldots \wedge s_n \Rightarrow q$ is a tautology.*

EXAMPLE 6.5. *Modus ponens.*

We need to show that the rule "From p and $p \Rightarrow q$, we may deduce q" is valid. So we consider the compound statement:

$$p \wedge (p \Rightarrow q) \Rightarrow q$$

It is easy to check with a truth table that this is a tautology. Since this is a tautology, the argument is valid.

EXAMPLE 6.6. *Proof by contradiction.*

Proof by contradiction is valid since the following is a tautology:

$$(\neg q \Rightarrow r \wedge \neg r) \Rightarrow q$$

A **fallacy** is an invalid argument which looks like it is a valid rule of inference.

EXAMPLE 6.7. *The following is a fallacy:*

> If Wayne likes computers, then Wayne is a nerd. Wayne is a nerd. Therefore, Wayne likes computers.

This has the form

$$(c \Rightarrow n) \wedge n \Rightarrow c$$

This statement is not a tautology: for example, it is false when c is false and n is true.

6.5 Predicates

We have seen statements that are either true or false. Often one has to deal with a more general situation where there are variables. For instance, in Example 6.7 we translated "Wayne like computers" as c. Now, if we are faced with the statement about Rincewind instead of Wayne, we have to redo things. It would be better to have a generic form that handles both situations simultaneously. In programming language terminology, rather than dealing with boolean variables, we now want to deal with boolean functions.

A **predicate** is what we need. For example, we might write $\mathit{like}(\text{Wayne}, \text{computers})$. Or we might write $\mathit{likeComp}(\text{Wayne})$, or even $\mathit{emotion}(\text{Wayne}, \text{like}, \text{computers})$. The exact choice of predicate depends on the situation and what seems appropriate at the time.

> Example 6.8. *Translate into predicates the argument: "If someone is a vegan then they have blue hair. Corin is a vegan. Therefore Corin has blue hair."*

If we have a predicate $\mathit{has}(x, y)$ for "x has y" and $\mathit{isa}(x, z)$ for "x is a z", we can write this as

$$\text{If } \mathit{isa}(x, \text{vegan}) \Rightarrow \mathit{has}(x, \text{blueHair}) \text{ and } \mathit{isa}(\text{Corin}, \text{vegan}), \text{ then } \mathit{has}(\text{Corin}, \text{blueHair}).$$

Note that I chose these exact predicates; you might easily choose other predicates.

But the above argument is potentially ambiguous, because we have not captured the idea that this applies only to people, and not say to zebras. It is better to specify the universes involve, which we consider next.

6.6 Quantifiers

We can write multiple statements as one statement using **quantifiers**. For example, in English we might write "the square of any number is nonnegative" or "all diseases will be cured by someone eventually". The quantifiers here are "any", "all", "someone" and "eventually" (if you think of this as "at some time").

Mathematics uses the following notation:

- $\forall$ for "for all", called the **universal quantifier**;
- $\exists$ for "there exists", the **existential quantifier**.

We will put parentheses around the expression that is subject to quantification. So we might write:

$$\forall m \, (m^2 \geq 0).$$

However, it is unclear whether the statement is true. It is true if we are thinking of m being an integer, but false if we allow m to be a complex number (since $i^2 = -1$). So we should really specify the universe (even though we often omit the universe if it is clear from context). Thus we write:

$$\forall m \in \mathbb{Z}\,(m^2 \geq 0).$$

The second example above, "all diseases will be cured by someone eventually", might be written as

$$\forall d \in \mathit{diseases}\,(\exists h \in \mathit{humans}\,(\exists t \in \mathit{time}\,(h \text{ cures } d \text{ at } t)))$$

I agree that this gets cumbersome quickly; but the point is that this does allow us to write down things in mathematical notation (and also to feed things into a computer for automated reasoning).

Example 6.9. *"There is no odd number whose square is even"*

This can be written as

$$\neg\,\exists x \in \mathbb{Z}\,(\,o(x) \wedge e(x^2)\,)$$

if we have predicates $o(y)$ meaning y is odd and $e(y)$ meaning y is even. Of course, we get different answers if we assume different predicates. (For example, we might define $s(y)$ for the square of y is even, or even use $\neg\,e(y)$ for being odd.)

Example 6.10. *Integer quotient and remainder*

We can express the existence of the quotient and remainder in integer division as "Given positive integer n and nonnegative integer m, there exist nonnegative integers q and r (quotient and remainder) such that $m = nq + r$ and $r < n$. This can be written in math-speak as

$$\forall n \in \mathbb{Z}^+\,(\forall m \in \mathbb{N}\,(\exists q \in \mathbb{N}\,(\exists r \in \mathbb{N}\,((m = nq + r) \wedge (r < n)))))$$

(I wrote this slowly, so that you can read it slowly…)

There is an intimate connection between $\forall$ and $\exists$ (which generalizes de Morgan's laws):

Lemma 6.1 *(a) The statement $\neg\,\forall x(p(x))$ is equivalent to $\exists x(\neg\,p(x))$.*
(b) The statement $\neg\,\exists x(p(x))$ is equivalent to $\forall x(\neg\,p(x))$.

If we let $p(x)$ stand for an arbitrary statement involving variable x, then to show that $\forall x(p(x))$ is false, it is sufficient to find one x where $p(x)$ is false (that is, a counterexample). Similarly, to show that $\exists x(p(x))$ is true, it is sufficient to find one x where $p(x)$ is true.

We can also use predicates and quantifiers in definitions. In these, there is a "free variable", meaning a variable that is not quantified. For example, to define an integer x as even we might say:

$$x \text{ is even if } \exists y \in \mathbb{Z}\,(x = 2y).$$

Exercises

6.1. Prove that the square of an even integer is a multiple of 4.

6.2. Show that the product of four consecutive integers is a multiple of 12.

6.3. Give a proof by contradiction that if x, y, z are integers such that $xyz \leq 1000$, then at least one of x, y, z is at most 10.

6.4. Give a **proof by contradiction** that for all real numbers x, if $x^2 - 2x \neq -1$, then $x \neq 1$.

6.5. Use proof by contradiction to show that if $x^2 + x - 2 = 0$ then $x \neq 0$.

6.6. Celia has a square piece of paper with each side two feet. Prove that if she draws 11 crosses on this paper, then at least one pair of crosses must be less than one foot apart.

6.7. Let p be a prime number other than 2. Prove that $2p$ cannot be written as the difference of squares (of integers).

6.8. (a) Prove that the sum of two rational numbers is rational.

(b) Prove by contradiction that the sum of a rational and an irrational number is irrational.

(c) What happens when you sum two irrational numbers?

6.9. (a) Suppose that there are 6 people in a room. Show that one can always find a group of 3 people such that either nobody in the group knows anybody in the group or everybody in the group knows everyone in the group.

(b) Show that this conclusion does not hold if there are only 5 people in the room.

6.10. Use proof by contradiction to prove that there are infinitely many prime numbers. (Hint: consider the number M that is 1 more than the product of all primes.)

6.11. Determine which of the following are valid rules of inference. Justify your answer.

(a) If $a \vee b$ and $a \Rightarrow c$ and $b \Rightarrow c$, then c.

(b) If $p \Rightarrow q$ and $\neg q$, then $\neg p$.

(c) If $a \Rightarrow b$ and $b \Rightarrow a$, then a.

(d) If $d \Rightarrow e$ and $e \Rightarrow f$, then $d \Rightarrow f$.

6.12. Convert to a quantified statement with predicates:

(a) Fridays are great!

(b) There is no largest integer.

6.13. Let $\mathbb{N}$ denote the set of nonnegative integers. Translate the following statements about $\mathbb{N}$ into English and then state whether they are true or false. Justify your answer.

(a) $\exists x\,(\forall y\,(x \geq y)\,)$

(b) $\forall x\,(\exists y\,(x > y)\,)$

(c) $\forall x\,(\forall y\,(\,(x \geq y) \vee (x \leq y)\,)\,)$

6.14. Use quantifiers to define a prime. That is, give a compound statement over the universe the integers with free variable x that is true exactly when x is a prime.

6.15. Negate and simplify the following:
$\forall x\,(\forall y\,((x < y) \Rightarrow \exists z(x < z < y)))$.
(There should be no $\neg$ in your final answer.)

6.16. Are the following pairs of statements equivalent?

(a) $\forall x\,(p(x))$ and $\neg\,\exists y\,(\neg\,p(y))$

(b) $\forall x\,(\forall y\,(q(x,y)))$ and $\forall y\,(\forall x\,(q(x,y)))$

(c) $\forall x\,(\exists y\,(r(x,y)))$ and $\exists y\,(\forall x\,(r(x,y)))$

(d) $\exists x\,(s(x) \wedge t(x))$ and $(\exists\,x(s(x)))\ \wedge\ (\exists\,x(t(x)))$

6.17. Using $s(x,y,z)$ to stand for the expression $x = yz$ and $t(x,y)$ to stand for the expression $x \leq y$, write down in logic what is means for d to be the greatest common divisor of m and n. (Assume the universe is the positive integers throughout.)

Solutions to Practice Exercises

1. Note that $x^2 - 1 = (x-1)(x+1)$. Since $x^2 - 1$ is a multiple of 3, it follows that either $x-1$ or $x+1$ is a multiple of 3. That is, it follows that x is either 1 less or 1 more than a multiple of 3, and in both cases, x is not a multiple of 3.

7 Automated Reasoning

In this section we consider a technique called resolution, which can be used to automate logical deductions.

7.1 Manipulating Logic Statements

It is tedious to establish logical equivalence using truth tables. Fortunately, one can often simplify statements by replacing one statement with an equivalent one. This uses various laws such as de Morgan's laws. One useful law is the **distributive law**. This comes in two versions:

$$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$$
$$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$$

EXAMPLE 7.1. *Simplify* $(p \land q) \lor (p \land \neg q)$.

$(p \land q) \lor (p \land \neg q) \equiv p \land (q \lor \neg q) \equiv p \land \mathsf{T} \equiv p$

It is also often useful to convert the statement into a special form. A statement is in **conjunctive normal form** if it is the **and** of clauses, where a **clause** is the **or** of variables or negated variables. For example,

$$(a \lor b \lor \neg c) \land (\neg d \lor c) \land (a \lor e)$$

is in conjunctive normal form. The distributive law is useful in converting a statement into conjunctive normal form. Indeed, any statement can be converted into this form, but the resulting statement might be very large.

7.2 Proof by Resolution

Resolution provides a strategy for automated proof. This is one of the ideas in automated theorem proving in AI. We present it here using only statements, but it can readily be extended to handle predicates. It forms the basis of the programming language Prolog.

Resolution is the rule of inference

"Given $a \lor b$ and $\neg b \lor c$, conclude $a \lor c$."

This is a valid rule of inference because $(a \vee b) \wedge (\neg b \vee c) \Rightarrow a \vee c$ is a tautology.

The basic idea in a proof using resolution is to convert every fact into a clause (that is, the **or** of variables or negated variables). Then repeatedly use the resolution rule to generate new facts until you get the fact you want. But actually, it is more efficient if we use proof by contradiction:

```
PROOF BY RESOLUTION
Convert all facts to clauses
Negate the theorem to be proved and add as fact
Repeat forever:
    if have pair of facts that have not had resolution applied to them, do it.
    if have no such pair of facts, then abort (the theorem is not provable).
    if reach contradiction, then theorem is proved.
```

EXAMPLE 7.2. *Prove Wayne is Fatuous from the following facts:*
If Wayne is Excellent, then Wayne is Keen
If Wayne is Laughable, then Wayne is not Keen
Wayne is Laughable
Wayne is Excellent or Fatuous

We can express this in logic as:
1. $e \Rightarrow k$
2. $l \Rightarrow \neg k$
3. l
4. $e \vee f$

The proof by resolution is then:
1. $\neg e \vee k$
2. $\neg l \vee \neg k$
3. l
4. $e \vee f$
5. $\neg f$ (opposite of theorem)
6. e 4&5
7. k 1&6
8. $\neg l$ 2&7
9. Contradiction 8&3

Note that one has to convert all given information into a list of clauses. This sometimes requires a bit of thought. However, most of these situations can be resolved by noting that if we have $a \wedge b$, this can be split into the two facts a and b. For example, $c \Rightarrow d \wedge e$ is actually the two facts $c \Rightarrow d$ and $c \Rightarrow e$.

Exercises

7.1. Simplify the following:

(a) $(p \wedge \neg q) \vee p$

(b) $\neg((\neg p \wedge q) \vee (\neg p \wedge \neg q)) \vee (p \wedge q)$

7.2. Use truth tables to show that $p \vee q \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$.

7.3. Use resolution to prove that P is true given the following:

1. $P \Rightarrow \neg Q$
2. $Q \vee S \Rightarrow \neg T$
3. $\neg S$
4. $R \Rightarrow P \vee Q$
5. $Q \vee R$
6. $S \vee T$

7.4. Use resolution to deduce that Q is false from the following:

1. $P \vee T$
2. $T \Rightarrow R$
3. $P \wedge S \Rightarrow \neg Q$
4. $\neg R$
5. $\neg T \Rightarrow S$

7.5. Use resolution to deduce that b is true from the following:

1. $a \Rightarrow b$
2. c
3. $d \vee e$
4. $e \Rightarrow b \vee \neg c$
5. $d \Rightarrow a \wedge f$

8 Primes and Modular Arithmetic

8.1 Primes and Factors

Over two millennia ago already, people all over the world were considering the properties of numbers. One of the simplest concepts is prime numbers. We use the notation $\mathbb{N}$ to denote the nonnegative integers. That is, $\mathbb{N} = \{0, 1, 2, \ldots\}$. Unless otherwise specified, we restrict our attention here to the set $\mathbb{N}$ throughout this chapter.

- We say a is a **factor** or **divisor** of b, and b is a **multiple** of a, if a goes into b without a remainder. For example, the factors of 6 are 1, 2, 3 and 6.
- A number greater than 1 with only itself and 1 as factors is called a **prime** number. Otherwise it is **composite**. (For the record, 1 is neither prime nor composite but is a **unit**.) For example, 19 is prime, but 21 is composite.
- The **gcd** (greatest common divisor) of two numbers, also known as the highest common factor, is the largest number that is a factor of both numbers. For example, $\gcd(6, 14) = 2$.
- Two numbers are **relatively prime** if they have no common factor apart from 1. That is, their gcd is 1.

If a number is composite, then it is a product of two nontrivial factors (nontrivial here meaning neither is 1). And these factors, if composite, are themselves products of factors. Eventually we reach primes. Thus any integer has a **prime factorization** (and the factorization is unique). For example, the prime factorization of 60 is $2^2 \times 3 \times 5$. This fact is sometimes called the "Fundamental Theorem of Arithmetic":

Theorem 8.1 *Every integer $a > 1$ can be expressed uniquely as a product of primes.*

While this theorem may sound obvious, if one is being careful, this fact actually needs several lines to prove it. The reason for the name of the theorem is that there are many places in mathematics where a form of multiplication is defined, and one of the first questions asked is about uniqueness of factoring.

8.2 Euclid's Algorithm

If we have the prime factorization of the two numbers, then there is a straightforward recipe to calculate their gcd:

> *take the smaller power of each common prime and multiply together.*

For example, consider $\gcd(36, 120)$. Since $36 = 2^2 \times 3^2$ and $120 = 2^3 \times 3 \times 5$, their gcd is $2^2 \times 3 = 12$.

Surprisingly, knowing the factorizations is not necessary, as was known to Euclid and other ancients. To explain this, we need to introduce a new operator called "mod".

Let d be a positive integer. For $c \in \mathbb{N}$, the value $c \bmod d$ is the remainder when c is divided by d. For example,

> $c \bmod d = 0$ if and only if d is a multiple of c.

Here is **Euclid's Algorithm** for the greatest common divisor of a and b:

```
GCD($a$,$b$)
    if $b$ is a factor of $a$, then return $b$
    else return $\gcd(b, a \bmod b)$
```

This is a recursive algorithm. The procedure is guaranteed to terminate, since the b-value decreases each time.

EXAMPLE 8.1. *What is the* gcd *of* 33 *and* 12*?*

$\gcd(33, 12) = \gcd(12, 9) = \gcd(9, 3) = 3$.

But we need to show that the procedure always gives the correct value.

If b is a factor of a, then clearly their gcd is b. So we need to show that when b is not a factor of a, that

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Well suppose $a = qb + r$ where $r = a \bmod b$. It follows that, if c is a factor of both b and r, then c is a factor of $qb + r$ as well, and so it is a factor of a. Conversely, we can re-arrange the equation to $r = a - qb$, and so if c is a factor of both a and b, then it is a factor of r as well. This shows that the set of common factors of a and b is the same as the set of common factors of a and r. In particular, the greatest element in the two sets must be the same.

Euclid's algorithm can be extended to prove the following result, and indeed to construct the s and t the theorem claims exist:

Theorem 8.2 *If c is the* gcd *of a and b, then there exist* integers *s and t such that*

$$s \times a + t \times b = c.$$

Example 8.2.

For 12 and 33, we have $3 \times 12 + (-1) \times 33 = 3$.

We omit the proof of the theorem.

▶ **For you to do!** ◀

1. *Use factorization to calculate the gcd of* 100 *and* 240.
2. *Use Euclid's algorithm to calculate the gcd of* 100 *and* 240.

8.3 Modular Addition and Multiplication

In arithmetic **modulo** n, when we add, subtract, or multiply two numbers, we take the answer mod n. For example, if we want the product of two numbers modulo n, then we multiply them normally and the answer is the remainder when the normal product is divided by n. The value n is sometimes called the **modulus**.

Specifically, let $\mathbb{Z}_n$ represent the set $\{0, 1, \ldots, n-1\}$ and define the two operations:

$$a +_n b = (a + b) \bmod n$$
$$a \cdot_n b = (a \times b) \bmod n$$

Modular arithmetic obeys the usual rules/laws for the operations addition and multiplication. For example, $a +_n b = b +_n a$ (commutative law) and $(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$ (associative law).

Now, we can write down **tables** for modular arithmetic. For example, here are the tables for arithmetic modulo 4 and modulo 5.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The table for addition is rather boring, and it changes in a rather obvious way if we change the modulus.

However, the table for multiplication is a bit more interesting. There is obviously a row with all zeroes. Consider the table for $\cdot_5$. Then in each of the other rows, every value is there and there is no repeated value. This does not always happen; for example, look at the table for modulus 4. Indeed, if both x and the modulus are a multiple of m, then every value in the row for x in the multiplication table will be a multiple of m. So the only way it can happen that all values appear in the multiplication table in every nonzero row is that the modulus is a prime. And in that case, yes this happens, as we now prove:

Theorem 8.3 *If p is a prime, and $1 \leq a \leq p-1$, then the values $0 \bmod p$, $a \bmod p$, $2a \bmod p$, $3a \bmod p$, …, $(p-1)a \bmod p$ are all distinct.*

Proof. Proof by contradiction. Suppose $ia \bmod p = ja \bmod p$ with $0 \leq i < j \leq p-1$. Then $(ja - ia) \bmod p = ja \bmod p - ia \bmod p = 0$, and so $ja - ia = (j-i)a$ is a multiple of p. However, a is not a multiple of p; so $j - i$ is a multiple of p. But that is impossible, because $j - i > 0$ and $j - i < p$. We have a contradiction. $\diamondsuit$

Since there are p distinct values in the row, but only p possible values, this means that every value must appear exactly once in the row.

We can also define **modular subtraction** in the same way, provided we say what the mod operation does when the first argument is negative: $c \bmod d$ is the smallest nonnegative number r such that $c = qd + r$ for some integer q; for example, $-1 \bmod d = d - 1$.

8.4 Modular Inverses

An interesting question is whether one can define division. This is based on the concept of an inverse, which is actually the more important concept. We define:

> *the* **inverse** *of b, written b^{-1}, is a number y in $\mathbb{Z}_n$ such that $b \cdot_n y = 1$.*

The question is: does such a y exist? And if so, how to find it? Well, it certainly does exist in some cases.

Example 8.3.

For $n = 7$, it holds that $4^{-1} = 2$ and $3^{-1} = 5$.

But 0^{-1} never exists.

Nevertheless, it turns out that modulo a prime p, all the remaining numbers have inverses. Actually, we already proved this when we showed in Theorem 8.3 that all values appear in a row of the multiplication table. In particular, we know that somewhere in the row for b there will be a 1; that is, there exists a y such that $b \cdot_p y = 1$.

And what about the case where the modulus is not a prime? For example, $7^{-1} = 13$ when the modulus is 15.

Theorem 8.4 *b^{-1} exists in $\mathbb{Z}_n$ if and only if b and n are relatively prime.*

Proof. There are two parts to prove. If b and n have a common factor say a, then any multiple of b is divisible by a and indeed $b \cdot_n y$ is a multiple of a for all y, so the inverse does not exist.

If b is relatively prime to n, then consider Euclid's extended algorithm. Given n and b, the algorithm behind Theorem 8.2 will produce integers x and y such that:

$$n \times x + b \times y = 1.$$

And so $b \cdot_n y = 1$. $\Diamond$

And, by using the extension of Euclid's algorithm, one actually has a quick algorithm for finding b^{-1}. One of the exercises is to show that if an inverse exists, then it is unique.

> ▶ **For you to do!** ◀
> *3. List all the values in $\mathbb{Z}_{11}$ and their inverses.*

8.5 Unsolved Problems

While we have come very far in number theory in thousands of years of effort, there are still many unsolved problems, some of which are easy to state. For example:

Conjecture 8.5 *(Goldbach's conjecture) Every even number at least 4 is the sum of two primes.*

Conjecture 8.6 *(Twin prime conjecture) There are infinitely many pairs of prime that differ only by 2 (such as 11 and 13).*

There is a lot of "evidence" to support Goldbach's conjecture. Indeed, it appears that as the even number get larger, it is the sum of two primes in many ways. But a proof remains elusive.

Another question is how to find the factors of a number. Is there an algorithm which runs in time proportional to some polynomial of the number of digits of a number and is guaranteed to find the factorization? Only recently did mankind find such an algorithm which tests whether a number is prime or composite (but the "proof" of compositeness does not find the factorization. . .).

Exercises

8.1. List all factors of 945.

8.2. How may factors are there of:

(a) 21

(b) $245,000$

(c) 2^{15}

8.3. Define $D(n)$ as the number of factors of n. For example, the primes are the n such that $D(n) = 2$.

(a) Determine all n such that $D(n) = 3$.

(b) Determine all n such that $D(n) = 4$.

8.4. A famous mathematician once noticed that the formula $f(n) = n^2 - n + 41$ yields primes for small values of n. For example, when $n = 1$ he calculated $f(1) = 41$, which is prime. When $n = 2$ he calculated $f(2) = 43$ and this is prime. Test the formula for $n = 3$, 4,and 5. Are the results prime? Does the formula always yield primes? Prove your answer.

8.5. Calculate the gcd of:

(a) 91 and 287.

(b) 12^{100} and 100^{12}.

8.6. Let a be a positive integer. Prove that $2a + 1$ and $4a^2 + 1$ are relatively prime.

8.7. Determine $\gcd(10^{10}, 20^{20})$.

8.8. Prove that if bc is a multiple of a and $\gcd(a, b) = 1$, then c is a multiple of a.

8.9. Show that the gcd operation is associative. That is: $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$.

8.10. (a) Write out the addition and multiplication tables for $\mathbb{Z}_2$.

(b) If we define 1 as true and 0 as false, explain which boolean connectives correspond to $+_2$ and $\cdot_2$.

8.11. Give the multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

8.12. Calculate 5^{-1} and 10^{-1} in $\mathbb{Z}_{17}$.

8.13. Prove that if b has an inverse in $\mathbb{Z}_n$, then it is unique.

8.14. How many elements of $\mathbb{Z}_{91}$ have multiplicative inverses in $\mathbb{Z}_{91}$?

8.15. How many rows of the table for $\cdot_{12}$ contain all values?

8.16. Consider $\mathbb{Z}_{10}$.

(a) List all elements of $\mathbb{Z}_{10}$.

(b) What is the inverse of 3?

(c) Give all square-roots of 6.

(d) How many rows of the multiplcation table contain every element?

8.17. (a) Consider the primes 5, 7, and 11 for n. For each integer from 1 through $n-1$, calculate its inverse.

(b) A number is **self-inverse** if it is its own inverse. For example, 1 is always self-inverse. Based on the data from (a), state a conjecture about the number of self-inverses when n is a prime.

(c) Prove your conjecture.

8.18. Given $a, b \in \mathbb{Z}_n$, we say that b is a **modular square-root** of a if $b \cdot_n b = a$.

(a) List all the elements in $\mathbb{Z}_{11}$, and for each element, list all their modular square-roots, if they have any.

(b) Prove that if n is prime then a has at most two square-roots.

(c) Give an example that shows that it is possible for a number to have **more** than 2 square-roots.

8.19. (a) Consider the primes 5, 7, and 11 for n. For each a from 1 through $n-1$, calculate $a^2 \bmod n$ (which is the same as $a \cdot_n a$).

(b) A number y is a **quadratic residue** if there is some a such that $y = a^2 \bmod n$. For example, 1 is always a quadratic residue (since it is $1^2 \bmod n$). Based on the data from (a), state a conjecture about the number of quadratic residues.

(c) Prove your conjecture.

Solutions to Practice Exercises

1. $100 = 2^2 \times 5^2$ and $240 = 2^3 \times 3 \times 5$. So gcd $= 2^2 \times 5 = 20$.

2. $(240, 100) \to (100, 40) \to (40, 20) \to 20$

3.

0	1	2	3	4	5	6	7	8	9	10
	1	6	4	3	9	2	8	7	5	10

9 Modular Exponentiation and Square-Roots

Modular arithmetic is used in cryptography. In particular, **modular exponentiation** is the cornerstone of what is called the RSA system.

9.1 Modular Exponentiation

We consider first an algorithm for calculating modular powers. The **modular exponentiation** problem is:

> compute $g^A \bmod n$, given g, A, and n.

The obvious algorithm to compute $g^A \bmod n$ multiplies g together A times. But there is a much faster algorithm to calculate $g^A \bmod n$, which uses at most $2 \log_2 A$ multiplications.

The algorithm uses the fact that one can reduce modulo n at each and every point. For example, that $ab \bmod n = (a \bmod n) \times (b \bmod n) \bmod n$. But the key savings is the insight that g^{2B} is the square of g^B.

```
DEXPO($g$,$A$,$n$)
    if $A = 0$ then return 1
    else if $A$ odd {
        $z$ = dexpo($g$, $A - 1$, $n$)
        return($zg \bmod n$)        % uses $g^A = g \times g^{A-1}$
        }
    else {
        $z$ = dexpo ($g$, $A/2$, $n$)
        return($z^2 \bmod n$)       % uses $g^A = (g^{A/2})^2$
        }
```

Note that the values of g and n are constant throughout the recursion. Further, at least every second turn the value of A is even and therefore is halved. Therefore the depth of recursion is at most $2 \log_2 A$.

We can do a modular exponentiation calculation by hand, by working out the sequence of values of A, and then calculating $g^A \bmod n$ for each of the A, starting with the smallest (which is $g^0 = 1$).

EXAMPLE 9.1. *Calculate* $3^{12} \bmod 5$.

A	$g^A \bmod n$
12	$4^2 \bmod 5 = 1$
6	$2^2 \bmod 5 = 1$
3	$3 \times 4 \bmod 5 = 2$
2	$3^2 \bmod 5 = 4$
1	$3 \times 1 \bmod 5 = 3$
0	1

▶ **For you to do!** ◀
1. Use the DEXPO *algorithm to calculate* $4^{14} \bmod 11$.

9.2 Modular Equations

A related question is trying to solve modular equations. These arise in puzzles where it says that: there was a collection of coconuts and when we divided it into four piles there was one left over, and when we divided it into five piles, etc.

Theorem 9.1 *Let $a \in \mathbb{N}$, and let b and c be positive integers that are relatively prime. Then the solution to the equation*

$$c \times x \bmod b = a$$

is all integers of the form $ib + a \cdot_b c^{-1}$ where i is an integer (which can be negative).

PROOF. We claim that the solution is all integers x such that $x \bmod b = a \cdot_b c^{-1}$, where c^{-1} is calculated modulo b. The proof of this is just to multiply both sides of the equation by c^{-1}, which we know exists. From there the result follows. ♢

EXAMPLE 9.2. *Solve the equation* $3x \bmod 10 = 4$.

Then $3^{-1} = 7$ and $4 \cdot_{10} 7 = 8$. So $x \bmod 10 = 8$.

This is then generalized in the Chinese Remainder Theorem. Here is just a special case:

Theorem 9.2 *If p and q are primes, then the solution to the pair of congruences*

$$x \equiv_p a \qquad \textit{and} \qquad x \equiv_q b$$

is all integers x such that

$$x \equiv_{pq} qaq^{-1} + pbp^{-1}$$

where p^{-1} is the inverse of p modulo q and q^{-1} is the inverse of q modulo p.

We omit the proof.

Example 9.3. *Determine all integers that have remainder* 2 *when divided by* 5 *and remainder* 4 *when divided by* 7.

In the notation of the above theorem, $a = 2$, $p = 5$, $b = 4$, and $q = 7$. In $\mathbb{Z}_7$, $5^{-1} = 3$. In $\mathbb{Z}_5$, $7^{-1} = 2^{-1} = 3$. So the set of solutions has remainder $7 \cdot 2 \cdot 3 + 5 \cdot 4 \cdot 3 \equiv_{35} 32$. So the answer is $35x + 32$ for x an integer.

9.3 Modular Exponentiation Theorems

We start with a famous theorem called **Fermat's Little Theorem**.

Theorem 9.3 *Fermat's little theorem. If p is a prime, then for a with $1 \le a \le p-1$,*

$$a^{p-1} \bmod p = 1.$$

Proof. Let S be the set $\{\, ia \bmod p : 1 \le i \le p-1 \,\}$. That is, multiply a by all integers in the range 1 to $p-1$ and write down the remainders when each is divided by p. Actually, we already looked at this set: it is the row corresponding to a from the multiplication table for p. And in Theorem 8.3 we showed that these values are all distinct. Therefore, S is actually just the set of integers from 1 up to $p-1$.

Now, let A be the product of the elements in S. To avoid ugly formulas, we use $x \equiv_p y$ to mean $x \bmod p = y \bmod p$. And we use Π-notation, which is the same as Σ-notation except that it is the product rather than the sum. By Theorem 8.3 and the above discussion,

$$\prod_{i=1}^{p-1} ((ia) \bmod p) = \prod_{i=1}^{p-1} i$$

But, we can also factor out the a's:

$$\prod_{i=1}^{p-1} (ia) \bmod p \equiv_p a^{p-1} \prod_{i=1}^{p-1} i$$

It follows that

$$\prod_{i=1}^{p-1} i \equiv_p a^{p-1} \prod_{i=1}^{p-1} i$$

Divide both sides by $\prod_{i-1}^{p-1} i$ and we get that $a^{p-1} \equiv_p 1$; that is, $a^{p-1} \bmod p = 1$. ♢

The above result is generalized by **Euler's Theorem**. We will need the following special case in the next chapter:

Theorem 9.4 *Special case of Euler's theorem. If a and $n = pq$ are relatively prime, with p and q distinct primes, then $a^{\phi} \bmod n = 1$ where $\phi = (p-1)(q-1)$.*

We omit the proof.

9.4 Square-Roots

Recall that in Exercise 8.18, we defined a **square-root** of a in $\mathbb{Z}_n$ as any element b such that $b^2 \bmod n$. Note that if b is a square-root, then so is $n - b$ (since $(n-b)^2 = n^2 - 2nb + b^2 \equiv_n b^2 \equiv_n a$). In the exercise you had to show that:

Lemma 9.5 *If n is any prime, then a has at most two square-roots modulo n.*

We will also need the following result in the next chapter:

Lemma 9.6 *If $n = pq$ where p and q are distinct primes, and one knows the square-roots of c modulo p and q, then one can find the square-roots of c modulo n.*

Proof. Let a_1, a_2 be the square-roots of c in $\mathbb{Z}_p$ and let b_1, b_2 be the square-roots of c in $\mathbb{Z}_q$, which we know. Further, let x be the square-root of c in $\mathbb{Z}_n$.

Then if we take $x \bmod p$ and square it in $\mathbb{Z}_p$, we get that $x^2 \equiv_p c$. That is, x (or at least its remainder) is a square-root of c in $\mathbb{Z}_p$ as well. Thus, we have that

$$x \equiv_p a_i \qquad \text{and} \qquad x \equiv_q b_j$$

for some $i \in \{1, 2\}$ and $j \in \{1, 2\}$. Thus, we need to solve a pair of congruences. For this, use Theorem 9.2. ♢

But that still raises the question of how to compute modular square-roots. Under certain circumstances, this can be done using modular exponentiation.

Theorem 9.7 *If p is a prime such that $p \bmod 4 = 3$, and* ***if*** *a has a square-root modulo p, then the square-roots of a are given by*

$$\pm a^{(p+1)/4} \bmod p$$

where $-x$ means $p - x$.

Proof. To show that $\pm a^{(p+1)/4}$ is a square-root, simply square it! Say b is one of the square-roots of a. That is, $b^2 \bmod p = a$. Then

$$\begin{aligned}\left(\pm a^{(p+1)/4}\right)^2 \bmod p &= a^{(p+1)/2} \bmod p \\ &= b^{(p+1)} \bmod p \\ &= b^{(p-1)} b^2 \bmod p \\ &= b^2 \bmod p \qquad \text{(By Fermat)} \\ &= a,\end{aligned}$$

as required. ◊

Example 9.4. *Consider square-roots modulo* 11.

The square-root of 3 is $\pm 3^3 \bmod 11$, which is 5 or 6.

Note that the theorem **assumed** the existence of a square-root. If we blindly exponentiate, things can be wrong: for example, it is not true that the square-roots of 2 modulo 11 are $\pm 2^3 \bmod 11$, which is 8 and 3. So one has to check whether the powers really are square-roots.

Exercises

9.1. (a) Compute $2^{38} \bmod 7$.

(b) Compute $3^{29} \bmod 20$.

(c) Compute $5^{33} \bmod 13$.

9.2. Describe all solutions to the modular equation $7x \bmod 8 = 3$.

9.3. Find the smallest positive solution to the set of modular equations:

$$x \bmod 3 = 2, \quad x \bmod 11 = 4, \quad x \bmod 8 = 7.$$

9.4. (a) Prove that $(a + b)^p \bmod p = (a^p + b^p) \bmod p$ if p is a prime.

(b) Use part (a) to give a proof of Fermat's Little Theorem.

9.5. Using the Binomial Theorem (and without using Fermat's Little Theorem), prove that for any odd prime p, it holds that $2^p \bmod p = 2$.

9.6. Let $a > 1$ be an integer.

(a) Show that $a^k - 1$ is a multiple $a - 1$ for any positive k.

(b) Show that if positive m and n are not relatively prime, then $a^m - 1$ and $a^n - 1$ are not relatively prime.

(c) Show that if positive m and n are relatively prime, then $a^m - 1$ and $a^n - 1$ are relatively prime.

9.7. (a) Show that if $n = pq$ for distinct primes p and q, then the number of integers from 1 up to n that are relatively prime to n is $(p-1)(q-1)$.

(b) Show that if $n = p^2$ for prime p, then the number of integers from 1 up to n that are relatively prime to n is $p(p-1)$.

(c) Generalize this. Let $\phi(n)$ be the number of values in $\mathbb{Z}_n$ that are relatively prime to n. Develop a formula for $\phi(n)$ based on the prime factorization of n.

9.8. Extend Theorem 9.7: prove that if p is a prime such that $p \bmod 4 = 3$, then $a^{(p+1)/4} \bmod p$ is always the square-root of either a or $p - a$.

Solutions to Practice Exercises

1.

A	$g^A \bmod n$
14	3
7	5
6	4
3	9
2	5
1	4
0	1

10 Modular Arithmetic in Cryptography

10.1 Encryption and Decryption

Encryption is used to send messages secretly. The sender has a message or **plaintext**. **Encryption** by the sender takes the plaintext and a **key** and produces **ciphertext**. **Decryption** by the receiver takes the ciphertext and a key and produces the plaintext. Ideally, encryption and decryption with the key should be easy, without the key it should be hard.

A famous idea is the **Caesar cipher**. Here the plaintext is written in letters. Then to encrypt it, we choose some small positive integer k, and replaces each letter by the letter k places along in the alphabet, with wrap around. For example, if the plaintext is the phrase `WAYNE RULES` and $k = 4$, then the ciphertext is `AECRI VYPIW` where spaces are left unchanged in this example.

In traditional cryptography, the encryption key has to be kept secret, since it is essentially the same as the decryption key. But in **public-key cryptography**, the two keys are related but in some way that is very difficult to get one from the other. So you can publish the one key and keep secret the other key. Indeed, this has been commercially exploited by RSA cryptosystems, formed by Rivest, Shamir, and Adleman.

10.2 RSA Described

Here is the original RSA cryptosystem. This allows Alice to send messages secretly to Bob. (Tradition requires that it is Alice and Bob.) That is, the ciphertext is unintelligible to anyone else.

1. Bob randomly picks two large distinct primes p and q.
2. Bob calculates $n = pq$ and $\phi = (p - 1)(q - 1)$.
3. Bob randomly picks some integer a with $1 \leq a < \phi$ such that a and ϕ are relatively prime.
4. Bob publishes n and a, and the public encryption function is $e(x) = x^a \bmod n$. That is, to send message M, Alice calculates and sends $M^a \bmod n$.
5. Bob uses the Extended Euclidean Algorithm to calculate $b = a^{-1}$ modulo ϕ.

6. The decryption function is $d(y) = y^b \bmod n$. That is, to decrypt message N, Bob calculates $N^b \bmod n$.

EXAMPLE 10.1. *A baby example.*

Take $p = 7$ and $q = 11$. Then $n = 77$ and $\phi(n) = 6 \times 10 = 60$. We need an a less than 60 that is relatively prime to 60; say $a = 13$. By the Extended Euclidean Algorithm (or a handy-dandy computer), $b = 37$.

If $M = 26$, then Alice calculates $y = 26^{13} \bmod 77 = 75$. Bob calculates $x = 75^{37} \bmod 77$, which equals 26.

We now show that RSA really works as a cryptosystem.

Theorem 10.1 *For all $M \in \mathbb{Z}_n$, $d(e(M)) = M$.*

PROOF. Well, let me first assume that M and n are relatively prime. Then, using the notation $x \equiv_n y$ to mean $x \bmod n = y \bmod n$,

$$\begin{aligned} d(e(M)) &\equiv_n (M^a)^b \\ &= M^{c\phi+1} \qquad \text{for some integer } c \\ &= (M^\phi)^c M \\ &\equiv_n M \qquad \text{by Theorem 9.4.} \end{aligned}$$

It can also be shown that the claim is true if M and n do have a common factor. But actually, in that case the cryptosystem has been broken, since then we have found a factor of n. ♢

10.3 Rabin's Public-Key Method

A year or so after RSA, Rabin introduced a related idea.

1. Bob chooses two large primes p and q such that $p \bmod 4 = q \bmod 4 = 3$. He calculates $n = pq$, and publishes n.
2. If M is Alice's plaintext, she calculates $N = M^2 \bmod n$ and sends that to Bob.
3. When Bob receives N, Bob calculates the square-roots of N modulo p by evaluating

$$a_1 = N^{(p+1)/4} \bmod p \qquad \text{and} \qquad b_1 = N^{(q+1)/4} \bmod q$$

   The square-roots of N modulo p are a_1 and $a_2 = p - a_1$ and the square-roots of N modulo q are b_1 and $b_2 = q - b_1$.

4. Bob determines the 4 possibilities for M by using the Chinese Remainder Theorem to solve the four sets of congruences:

$$M \equiv_p a_i \qquad \text{and} \qquad M \equiv_q b_i$$

And **hopefully** Bob can distinguish the real message from the three options that are garbage.

EXAMPLE 10.2. *A baby example.*

Suppose Bob chooses $p = 3$ and $q = 11$. Then $n = 33$.

Suppose Alice's plaintext is 8. Then Alice calculates $8^2 \bmod 33 = 31$.

Bob receives $N = 31$. He first finds a square-root of 31 modulo 3. He applies the above formula. That is, the square-roots are $\pm 31^1 \bmod 3 = 1, 2$. Bob then finds the square-root of 31 modulo 11. Applying the above formula, the square-roots are $\pm 31^3 \bmod 11 = 3, 8$.

Then Bob solves four sets of congruences. The first is: $M \equiv_3 1$ and $M \equiv_{11} 3$.
Applying the formula in Theorem 9.2, 3^{-1} modulo 11 is 4, and 11^{-1} modulo 3 is 2. Thus $M \equiv_n 11 \cdot 1 \cdot 2 + 3 \cdot 4 \cdot 3 = 58 \equiv_n 25$.

The other sets of congruences are: $M \equiv_3 1$ and $M \equiv_{11} 8$ which yields $M = 19$; $M \equiv_3 2$ and $M \equiv_{11} 3$ which yields $M = 14$; and $M \equiv_3 2$ and $M \equiv_{11} 8$ which yields $M = 8$.

Hopefully, it is clear to you that if one can factor quickly, then both RSA and Rabin are breakable. The converse has been shown for Rabin; that is, if you can break Rabin quickly, then you can factor quickly.

Exercises

10.1. Take $p = 5$, $q = 11$ and $a = 27$ in RSA. Verify that $b = 3$. If $M = 4$, what does Alice send? If Bob receives 9, what was M?

10.2. Take $p = 11$, $q = 13$ and $a = 37$ in RSA. Verify that $b = 13$. If $M = 62$, what does Alice send?

10.3. Take $n = 65$ and $a = 11$ in RSA. Determine b. If $M = 2$, determine what Alice sends.

10.4. Beth sets up a Rabin system with public key 77.

(a) If Alain's plaintext is 10, what does he send?

(b) Calculate the square roots of 4 in $\mathbb{Z}_7$ and in $\mathbb{Z}_{11}$.

(c) If Beth receives 4, give at least two possibilities for Alain's plaintext.

11 Mathematical Induction

The principle of **mathematical induction** rests on the following idea. Assume $p(n)$ is some predicate about an integer n:

> **Mathematical Induction.** *If statement $p(b)$ is true, and*
> *statement $p(n-1) \Rightarrow p(n)$ is true for all $n > b$,*
> *then $p(n)$ is true for all integers $n \geq b$.*

The justification is that by the first part we have that $p(b)$ is true. Then by the second part we have that $p(b+1)$ is true. Then by the second part we have that $p(b+2)$ is true. And so on.

There is a standard recipe for proofs using mathematical induction. We first prove the **base case**. Then we assume $p(n-1)$ is true—called the **inductive hypothesis** and abbreviated IH—and using this fact, we prove that $p(n)$ is true. In this course, many of our examples are proving formulas. In this case, we use LHS to stand for the left-hand side, and RHS for the right-hand-side.

Example 11.1. *Prove that $1 + 2 + 3 + \ldots + n = n(n+1)/2$ for all $n \geq 1$.*

Base case: When $n = 1$, LHS = 1; RHS = $1(1+1)/2 = 1$; so LHS = RHS.

Inductive step: Assume formula true for $n-1$; show for n. Then

$$\begin{aligned} \text{LHS} &= 1 + 2 + 3 + \ldots + n \\ &= [1 + 2 + 3 + \ldots + n - 1]\ + n \\ &= \frac{(n-1)((n-1)+1)}{2} \ + \ n \quad \text{by IH} \\ &= \frac{(n-1)n + 2n}{2} \\ &= \frac{n(n+1)}{2} \\ &= \text{RHS} \end{aligned}$$

Thus the formula is true for all $n \geq 1$.

When proving formulas for sums, we often use this "peeling" idea; that is, we take the whole sum and separate out the part for $n-1$.

Example 11.2. *Prove by induction for all $n \geq 0$, that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.*

Base case: When $n = 0$, LHS $= 2^0 = 1$; RHS $= 2^1 - 1 = 1$; so LHS = RHS.

Inductive step: Assume formula true for $n - 1$; show for n. Then

$$\begin{aligned}
\text{LHS} &= \sum_{i=0}^{n} 2^i \\
&= \sum_{i=0}^{n-1} 2^i \ + 2^n \\
&= 2^n - 1 \ + 2^n \quad \text{by IH} \\
&= 2^{n+1} - 1 \\
&= \text{RHS}
\end{aligned}$$

Thus the formula is true for all $n \geq 0$.

Example 11.3. *Prove that $2^{n+1} > n^2 + 3$ for all $n \geq 2$.*

Base case: When $n = 2$, LHS $= 2^3 = 8$, and RHS $= n^2 + 3 = 7$, so statement true for $n = 2$.

Inductive step: Assume $n > 2$ and statement true for $n - 1$; that is, $2^n > (n-1)^2 + 3$. We want to show that $2^{n+1} > n^2 + 3$. Then

$$\begin{aligned}
\text{LHS} = 2^{n+1} &= 2 \times 2^n \\
&> 2 \times \big((n-1)^2 + 3\big) \qquad \text{by IH} \\
&= 2(n^2 - 2n + 4) \\
&= 2n^2 - 4n + 8 \\
&= \big(n^2 + 3\big) + \big((n-2)^2 + 1\big) \\
&> n^2 + 3 = \text{RHS}
\end{aligned}$$

as required. Therefore, the result is true by mathematical induction.

Example 11.4. *Show that $2^n + 3^n$ is a multiple of 5 for all positive odd integers n.*

Base case: When $n = 1$, $2^1 + 3^1 = 5$, which is a multiple of 5.

Inductive step: Let $n = 2i + 1$. Assume true for $i - 1$, test for i. Then

$$2^{2i+1} + 3^{2i+1} = 4 \times 2^{2i-1} + 9 \times 3^{2i-1} = 4 \times (2^{2i-1} + 3^{2i-1}) + 5 \times 3^{2i-1}.$$

The first term is a multiple of 5 by the IH. The second term is a multiple of 5 too. Therefore the sum is a multiple of 5. Hence $2^n + 3^n$ is a multiple of 5.

In **strong induction**, the inductive step is replaced by the following:

$$p(b) \wedge p(b+1) \wedge \cdots \wedge p(n-1) \Rightarrow p(n)$$

But we do not need that here.

▶ **For you to do!** ◀

1. Prove that $1 \times 2 + 2 \times 3 + 3 \times 4 + \ldots + (n-1) \times n = \frac{n^3-n}{3}$ *for all* $n \geq 2$.

Exercises

11.1. Prove that $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$ for all $n \geq 1$.

11.2. Prove by induction that for all $n \geq 1$

$$\sum_{i=1}^{n} i\,2^i = (n-1)2^{n+1} + 2.$$

11.3. Prove by induction that for all $n \geq 1$:

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

11.4. Prove that $n! > 2^n$ for $n \geq 4$.

11.5. Prove by induction that $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$.

11.6. Prove by induction a formula for $\sum_{i=1}^{n} i^3$. (Hint: it is a polynomial of degree 4.)

11.7. Prove by induction that for all $n \geq 1$

$$\sum_{i=1}^{n} (-1)^i\, i^2 = \frac{(-1)^n n(n+1)}{2}$$

(Note that the sum starts $-1 + 4 - 9 + 16 \ldots$.)

11.8. Winifred wants the formula for

$$\sum_{i=1}^{n} i^2 2^i$$

(That is, $1 \times 2^1 + 4 \times 2^2 + 9 \times 2^3 + 16 \times 2^4 \ldots$) She finds the formula in a book, except that someone has smeared a bit of ink on it. The result is that the formula reads

$$(n^2 - 2n + \circledast)2^{n+1} - \circledast$$

Determine what the two $\circledast$'s are. (Hint: each is a (different) positive integer.)

11.9. Prove by induction that $3^n \geq n^3$ for all integers $n \geq 3$.

11.10. Prove that $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$ for all integers $n \geq 1$.

11.11. Prove by induction that for every positive integer n, $4^{2n+1} + 11^n$ is divisible by 5.

11.12. Prove by induction that for every positive integer n, $6^{2n+1} + 4^{3n}$ is divisible by 7.

11.13. Prove that the sum of the interior angles of an n-gon is $(n-2)180$ degrees.

11.14. Prove that $\sum_{i=1}^{\infty} \frac{1}{i}$ is infinite. (Hint: show by induction that $\sum_{i=1}^{2^k} \frac{1}{i} \geq k/2$.)

11.15. Prove by induction that there are at least n primes for all positive integers n. (That is, there are infinitely many primes.)

11.16. Consider a prison which is the shape of an n-gon (not necessarily convex). The warden has three teams of guards, a red team, a blue team, and a green team. The warder wants to assign each vertex of the polygon to one (guard of a) specific team, such that every point in the interior of the polygon is visible to (at least one member of) each team.

(a) Prove by induction that this is possible.

(b) Construct a 100-gon prison where, if we have to leave one of the vertices unassigned, then it is not possible to satisfy the warden's requirements.

11.17. Using the Internet, write a page on the Unexpected Hanging Paradox.

Solutions to Practice Exercises

1. *Base case:* LHS $= 1 \times 2 = 2$; RHS $= (2^3 - 2)/2 = 2$; so LHS = RHS.

Inductive step: Assume formula true for $n-1$; show for n. Then

$$\begin{aligned}
\text{LHS} &= 1 \times 2 + 2 \times 3 + 3 \times 4 + \ldots + (n-1) \times n \\
&= [1 \times 2 + 2 \times 3 + 3 \times 4 + \ldots + (n-2)(n-1)] + (n-1) \times n \\
&= \frac{(n-1)^3 - (n-1)}{3} + (n-1)n \quad \text{by IH} \\
&= \frac{n-1}{3}\left[(n-1)^2 - 1 + 3n\right] \\
&= \frac{n-1}{3}\left[n^2 + n\right] \\
&= \text{RHS}
\end{aligned}$$

12 Sequences and Recurrences

A sequence is just what you think it is. It is often given by a formula known as a recurrence equation.

12.1 Arithmetic and Geometric Progressions

An **arithmetic progression** is a sequence where every two consecutive entries differ by the same amount. For example,

$$4, 7, 10, 13, 16, \ldots$$

If the sequence has first term A and last term L and there are n terms in the sequence, then an arithmetic progression has sum

$$\frac{n(A+L)}{2}$$

(Proof left as exercise.)

A **geometric progression** is a sequence where every two consecutive entries have the same ratio. For example,

$$2, 6, 18, 54, 162, \ldots$$

A useful fact is the sum of a geometric progression:

$$\sum_{i=0}^{n-1} Ar^i = \frac{A(r^n - 1)}{r - 1}$$

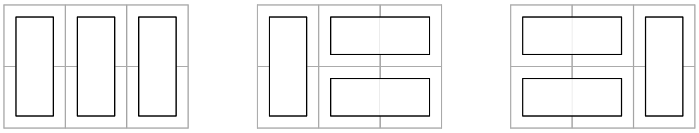
provided $r \neq 1$. This can be proved by induction, or by this idea:

$$r \cdot \text{LHS} = \sum_{i=0}^{n-1} Ar^{i+1} = \sum_{i=1}^{n} Ar^i = \text{LHS} + Ar^n - A,$$

so that $(r-1)\text{LHS} = A(r^n - 1)$.

12.2 Fibonacci Numbers

Consider a board like a checkerboard that is partitioned into squares. Define a tiling of a board to mean covering the board completely with nonoverlapping dominoes, where each domino covers two adjacent squares. Consider a board with 2 rows and n columns. Clearly, there is a tiling with all vertical dominoes. But how many tilings are there? For example, if there are 3 columns, there are two other tilings, each with only 1 vertical domino:



Let $f(n)$ be the number of domino tilings of the $2 \times n$ board. Let's look for a way of writing $f(n)$ in terms of smaller values. The idea is to look at the left end of the board. There are two possibilities: either there is a vertical domino at the left, or there are two horizontal dominoes. In the first case, the remaining dominoes form a tiling of the $2 \times (n-1)$ board; in the second case, the remaining dominoes form a tiling of the $2 \times (n-2)$ board. By the sum rule, we thus have:

$$f(n) = f(n-1) + f(n-2).$$

If there is only 1 column, then the recurrence formula breaks down, as two horizontal dominoes are impossible. If there are 2 columns, then the recurrence formula is valid, provided one defines $f(0) = 1$.

With some paper, one can calculate $f(n)$, starting with $f(0)$:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

These are the famous Fibonacci numbers. Gazillion things are counted by these.

They also have many patterns—here is one example.

Theorem 12.1 *For all $n \geq 1$,*

$$[f(n)]^2 - f(n-1)f(n+1) = (-1)^n.$$

Proof. Proof by mathematical induction. The base case is $n = 1$. LHS $= [f(1)]^2 - f(0)f(2) = 1^2 - 1 \cdot 2 = -1$. RHS $= (-1)^1 = -1$. So the base case is true.

Now for the induction step. *Assume* the statement is true for $n-1$; we need to prove it for n. Well, start with the LHS for that case, use the definition of the Fibonacci sequence, and do some algebra:

$$\begin{aligned}
\text{LHS} &= [f(n)]^2 - f(n-1)f(n+1) \\
&= f(n)[f(n-1) + f(n-2)] - f(n-1)[f(n) + f(n-1)] \qquad \text{(by Fibonacci defn twice)} \\
&= f(n)f(n-2) - f(n-1)f(n-1) \qquad \text{(by simplification)} \\
&= -(-1)^{n-1} \qquad \text{(by the induction hypothesis)} \\
&= (-1)^n = \text{RHS},
\end{aligned}$$

as required. $\Diamond$

The original story behind the Fibonacci numbers was the following: A pair of rabbits starts breeding after two months and produces one pair every month thereafter. Assume we start with one new-born pair of rabbits. Let $R(n)$ be the number of pairs of rabbits after n months. Then we claim that

$$R(n) = R(n-1) + R(n-2)$$

with $R(0) = R(1) = 1$. For, we still have the rabbits we had the month before. And every pair that is at least two months old produces a new pair. The number that are two months old are the ones that were alive two months ago.

There is a weird-looking formula for Fibonacci numbers:

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

We shall see where this comes from in a moment.

12.3 Recurrence Equations

The formula for the Fibonacci numbers is an example of a recurrence. Here is another example.

Example 12.1. *Find a recurrence for $S(n)$, the number of subsets of $\{1, 2, 3, \ldots, n\}$.*

Every subset of $\{1, 2, \ldots, n-1\}$ can be extended to a subset of $\{1, 2, 3, \ldots, n\}$ by either adding or not adding the element n. Therefore

$S(n) = 2S(n-1)$ for $n \geq 1$ and $S(0) = 1$.

It follows immediately that $S(n) = 2^n$.

Most recurrence relations have **initial conditions**, since the recursive formula breaks down eventually for the smallest n. Note that without knowing the initial condition, the recurrence $S(n) = 2S(n-1)$ has multiple solutions: $S(n) = \alpha 2^n$ is a solution for any real number α (including zero!). One can **verify** that some formula is a solution by plugging it into both sides and checking that one gets the same value. (Do it here!)

Example 12.2. *Find a recurrence for $P(n)$, the number of unordered pairs from the set $\{1, 2, 3, \ldots, n\}$.*

We saw already that $P(n) = \binom{n}{2}$. But we can obtain a recurrence. Partition the pairs into two sets based on whether they contain the element n or not. There are $n-1$ pairs that contain element n, and $P(n-1)$ that don't. So

$$P(n) = n - 1 + P(n-1)$$

with initial condition $P(1) = 0$.

Example 12.3. *My money A is invested at interest rate of p percent compounding annually. What do I have after n years?*

Let $M(n)$ be the amount after n years. Then $M(n) = (1+p/100)M(n-1)$, with $M(0) = A$.

12.4 Iterating the Recurrence

We can solve some recurrences by iterating them. This means repeatedly using the recurrence relation to re-write the RHS. (Actually, we can often get some information about them this way.)

For example: For our money from Example 12.3:

$$M(n) = (1+p/100)M(n-1) = (1+p/100)^2 M(n-2) = \ldots = (1+p/100)^n A.$$

And for our pairs from Example 12.2:

$$P(n) = (n-1) + (n-2) + \ldots 1 + 0 = n(n-1)/2$$

where the last part uses the formula for the sum of an arithmetic progression.

Here is a harder example of solving a recurrence using iteration.

Example 12.4. *Solve*

$$T(n) = 4T(n-1) + 2^n \qquad \text{with } T(0) = 6.$$

Iterating the recurrence:

$$\begin{aligned}
T(n) &= 2^n + 4T(n-1) \\
&= 2^n + 4(2^{n-1} + 4T(n-2)) \\
&= 2^n + 2^{n+1} + 4^2 T(n-2) \\
&= 2^n + 2^{n+1} + 2^{n+2} + 4^3 T(n-3) \\
&= \ldots \\
&= \left(2^n + 2^{n+1} + \ldots 2^{2n-1}\right) + 4^n T(0) \\
&= (2^{2n} - 2^n) + 6 \cdot 4^n \\
&= 7 \cdot 4^n - 2^n
\end{aligned}$$

12.5 More Recurrences

A string of parentheses is called **valid** if it is of the correct form for an arithmetic expression. That is, the parentheses pair off such that every two pairs either nest or don't overlap at all. For example, there are two valid strings of 4 parentheses: `(())` and `()()`. (The valid strings have the property that, reading left to right, the number of left parentheses is always at least the number of right parentheses.)

Let $p(n)$ be the number of valid strings using $2n$ parentheses. This has a slightly more interesting recurrence:

$$p(n) = \sum_{i=1}^{n} p(i-1) \times p(n-i) \qquad (n \geq 1),$$

with $p(0) = 1$.

To prove the recurrence. Consider any valid string of parentheses. Then the parentheses pair off. Consider the first parenthesis (a left one) and its partner. Suppose that it partners with the i^{th} right parenthesis. Then the string A between these two is itself a valid string of length $2(i-1)$, and the string B after the partner is also a valid string of length $2(n-i-1)$. Conversely, if you give me any two strings of valid parentheses of combined length $2(n-1)$, I can recreate one of length $2(n)$ by $(A)B$. It follows that the number of strings of valid parentheses where the first parenthesis pair off with the i^{th} right parenthesis equals $p(i-1) \times p(n-i)$. If we sum over all i, we get the recurrence.

This solves to

$$p(n) = \frac{1}{n+1}\binom{2n}{n}$$

While we don't show how to find the solution, you can verify the solution yourself.

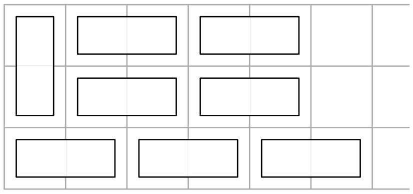
Example 12.5. *Find a recurrence for the number of domino tilings of a board with* 3 *rows and* $2m$ *columns.*

Let $t(m)$ be the number of such tilings. (Note that the number of columns has to be even for such a tiling to exist.) There are two possibilities for the first column.

(1) *All the dominoes are horizontal.* Then they stretch over into the second column as well. What remains is a $3 \times (2m-2)$ board. That is, the number of such possibilities is $t(m-1)$.

(2) *One domino is horizontal and one vertical.* The horizontal domino is either the top or the bottom row. This gives a factor of 2. Say the horizontal domino is in the bottom row.

Then look at the top two rows. If the dominoes in the second column are horizontal, they force another horizontal domino in the bottom row. This keeps on going until eventually there is a vertical domino in the top two rows.



This can take 2, 4, 6 etc or even all the columns. Thus the number of possibilities for this case is $2\,(t(m-1) + t(m-2) + t(m-3) + \ldots + t(1) + t(0))$, where we have defined $t(0) = 1$. Thus one gets the recurrence

$$t(m) = 3t(m-1) + 2t(m-2) + 2t(m-3) + \ldots + 2t(1) + 2t(0)$$

One can also use this to find a simpler-looking recurrence: take the equivalent recurrence for $t(m+1)$, that is $t(m+1) = 3t(m) + 2\sum_{i=0}^{m-1} t(i)$, and subtract these two recurrences. Then we get $t(m+1) - t(m) = 3t(m) - t(m-1)$, which simplifies to

$$t(m+1) = 4t(m) - t(m-1)$$

For example, we get 1, 3, 11, 41, 153, ...

12.6 Solving Recurrence Relations with Characteristic Equations

The recurrence relation for the Fibonacci numbers is a **second-order** recurrence, meaning it involves the previous **two** values. It is also **linear homogeneous**, meaning that every term is a constant multiplied by a sequence value. In general, one can write this as:

$$g(n) = ag(n-1) + bg(n-2).$$

Now, it turns out that $g(n) = r^n$—where r is some fixed real number—is a solution to this recurrence under certain circumstances. What are those circumstances? Well, a trivial case is $r = 0$; but let's assume $r \neq 0$. One can plug this alleged solution into both sides and see what must happen. The LHS is r^n. The RHS is $ar^{n-1} + br^{n-2}$. If we divide through by r^{n-2} (legal since $r \neq 0$), we get that $r^2 = ar + b$. Put another way, we need r to be a root (that is, a solution) of the following equation:

$$x^2 = ax + b.$$

This is called the **characteristic equation**.

Theorem 12.2 *If the characteristic equation $x^2 = ax + b$ has two distinct real roots r_1 and r_2, then the solution of the recurrence relation $g(n) = ag(n-1) + bg(n-2)$ $(n \geq 2)$ is given by*

$$g(n) = \alpha r_1^n + \beta r_2^n,$$

where α and β are real numbers.

Proof. We have just shown that each of $g(n) = r_1^n$ and $g(n) = r_2^n$ is a solution. The theorem claims that these two functions are, in the terms of linear algebra, a **basis** for the solution space: every other solution is a linear combination of these two, and every linear combination of these two is indeed a solution. We omit the proof, but you should do it if you need the exercise. $\diamondsuit$

Example 12.6. *Solve the recurrence $R(n) = 5R(n-1) - 6R(n-2)$.*

Method: the above theorem applies. The characteristic equation is $x^2 = 5x - 6$. We first solve the quadratic: the roots are $r_1 = 2$, $r_2 = 3$. So the general formula is $R(n) = \alpha 2^n + \beta 3^n$ for some constants α and β. The constants α and β can be obtained by looking at the initial conditions, which are the first two values of the sequence. We get two equations in two unknowns, which we then solve.

Let's determine the solution for the the Fibonacci numbers. The characteristic equation is $x^2 = x + 1$. By the quadratic formula, the roots of this are $r_1 = (1+\sqrt{5})/2$ and $r_2 = (1-\sqrt{5})/2$. So the solution is $f(n) = \alpha r_1^n + \beta r_2^n$.

The coefficients α and β are found by using the initial conditions, that is, that $f(0) = f(1) = 1$. In particular, we need that

$$f(0) = \alpha + \beta = 1 \quad \text{and} \quad f(1) = \alpha r_1 + \beta r_2 = 1.$$

And we get from algebra, that $\alpha = r_1/\sqrt{5}$ and $\beta = -r_2/\sqrt{5}$. This means that

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

But things are actually simpler than they look: as $n \to \infty$ the second term tends to zero, so actually

$$f(n) \approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1}.$$

(Indeed, it can be shown that $f(n)$ is the nearest integer to this quantity.)

One can also establish a similar result to the above theorem for the case where the two roots are not real, or for the case where there is a repeated root. The ideas for the latter are discussed in the exercises.

Exercises

12.1. Prove that if an n-term arithmetic progression has first term A and last-term L, then its sum is $n(A+L)/2$.

12.2. Consider a board like a checkerboard that is partitioned into squares. Define a tromino tiling of a board to mean covering the board completely with nonoverlapping trominoes, where each tromino covers three squares in a row (horizontally or vertically). Let $t(n)$ be the number of tromino tilings of the $3 \times n$ board. Give a recurrence formula for $t(n)$.

12.3. In a rabbit warren, each pair of rabbits aged two months or more produces 2 pairs per month (and never dies). If we start with 1 newborn pair, how many rabbits do we have after one year? After n years?

12.4. Prove by induction that the Fibonacci number $f(4m-1)$ is a multiple of 3 for all $m \geq 1$.

12.5. Let $S(n)$ be the number of strings of length n consisting of `0`s and `1`s such that no two `1`s are consecutive. Determine a recurrence formula for $S(n)$.

12.6. Prove that the Fibonacci sequence obeys the following identity:

$$f(0) + f(1) + \ldots + f(n) = f(n+2) - 1.$$

12.7. Prove that the Fibonacci numbers obey the following identity:

$$\sum_{i=0}^{n} [f(i)]^2 = f(n)f(n+1) \qquad \text{for } n \geq 0.$$

12.8. Prove that every positive integer can be written as a sum of some distinct Fibonacci numbers with the added restriction that no two of the Fibonacci numbers used are consecutive. For example, $28 = f(7) + f(4) + f(2)$.

12.9. (a) Show that any two consecutive Fibonacci numbers $f(n-1)$ and $f(n)$ are relatively prime.

(b) Code up or apply the Extended Euclid algorithm to find s and t such that $sf(n) + tf(n-1) = 1$. Discuss your results, conjecture a pattern, and try to prove your conjecture.

12.10. Verify that the formula for $p(n)$, the number of valid strings of $2n$ parentheses, is correct by showing that it satisfies the recurrence.

12.11. Wayne has a membership at the FoolTiltPoker website that allows him to play any days that he likes, except that he **can never play on three consecutive days**. Let $p(n)$ be the number of possible subsets of days in an n-day period when Wayne can play.

(a) Explain why $p(3) = 7$.

(b) Calculate $p(4)$.

(c) Give a recurrence for $p(n)$.

12.12. Solve the recurrence $z(n) = 2z(n-1) + 4^n$ with $z(0) = 1$ by iterating the recurrence.

12.13. Solve the recurrence $s(n) = 3s(n-1) + 1$ with $s(0) = 1$ by iterating the recurrence.

12.14. The Lucas numbers $l(n)$ are like the Fibonacci numbers, except that they start differently: 2, 1, 3, 4, 7, 11, 18 … State and prove a formula for the sum of the first n Lucas numbers.

12.15. Determine a formula for the Lucas numbers $l(n)$.

12.16. Give the general solution of the recurrence $g(n) = 2g(n-1) + 3g(n-2)$ by using the characteristic equation.

12.17. Solve the recurrence $h(n) = 6h(n-1) - 8h(n-2)$, with $h(1) =$ and $h(2) = 16$, by using the characteristic equation.

12.18. Consider the recurrence $h(n) = 4h(n-1) + 4h(n-2)$ $(n \geq 2)$.

(a) Show that the characteristic equation has only one root.

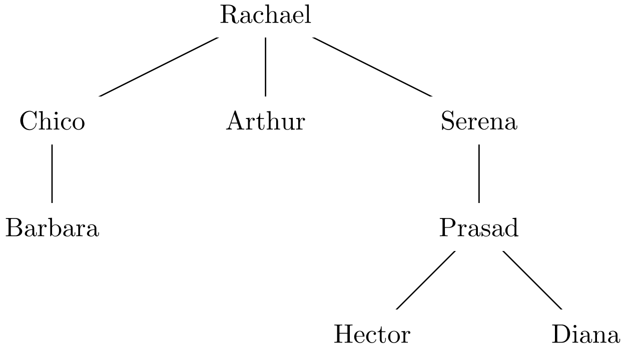
(b) Show that both $h(n) = 2^n$ and $h(n) = n2^n$ are solutions to the recurrence.

(c) Suppose $h(0) = 1$ and $h(1) = 2$. Solve the recurrence.

13 Trees and Graphs

13.1 Rooted and Unrooted Trees

We've all seen trees. No, not that sprightly spruce in your garden, but your family tree.



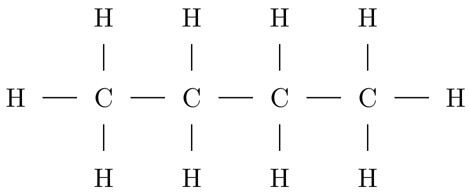
A tree consists of a collection of **vertices**, some of which are joined by **edges**. A **rooted tree** is a tree with one vertex designated the **root**. Rooted trees are normally drawn with the root at the top. The above example has 8 vertices, with Rachael the root.

For a rooted tree, we can talk of **parents** and **children** in the natural way. There are many other places that a rooted tree arises. One is the folder/directory structure on your computer. A parent directory contains child subdirectories. That tree is often drawn with the root on the top left and the branches growing left to right.

In general, a **tree** is just like a rooted tree, except it does not have a special vertex. A tree can also be defined recursively:

> *A single vertex is a tree;*
> *Adding one new vertex and joining it to one vertex of a tree yields a tree.*

For example, **alkanes** are chemical molecules consisting of carbon and hydrogen atoms, where each carbon atom has four bonds and each hydrogen atom has one bond. Specifically, all links are single bonds and there are no cycles or loops. So, here is a representation of *butane*: four carbons and ten hydrogen.



For mathematical purposes, one can suppress the hydrogen atoms, since we can always infer where they go. Chemists care about how many different **isomers** occur for a particular alkane. This is equivalent to counting the trees that can be made up of the carbon atoms. For example, there is only one isomer of methane, ethane and propane (which have 1, 2, and 3 carbon atoms respectively), but there are two isomers of butane.

▶ **For you to do!** ◀

1. Draw the other isomer of butane.

13.2 Graphs

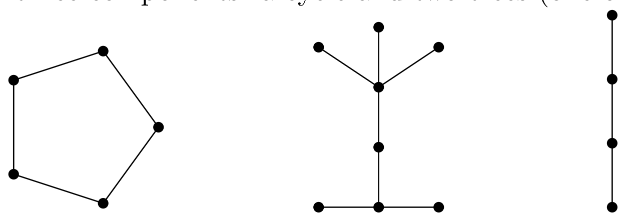
A (simple) **graph** is a collection of vertices and edges such that each edge joins two vertices. People sometimes allow **multiple edges** between vertices (for example, to represent double-bonds) or **loops** (edges both of whose ends are the same vertex), but we exclude those here—that is the meaning of “simple” in simple graph.

A typical place where a graph arises is with a map: the cities are the vertices; the roads are the edges. In this situation, the point is that the graph abstracts everything one needs to know. The actual direction or location of the road doesn’t matter; all we care about is how long does it take to traverse that road. Another graph is used in project planning: the vertices are the tasks, and there is a directed edge (we call this an **arc**) from one task to another if the first has to be completed before the second one starts. This allows for scheduling of resources, and also for critical path analysis, which tells one whether a particular task running late would cause the whole project to be delayed. Another (very large) graph is the Internet.

We need some terminology for graphs. A **walk** is a sequence of vertices such that consecutive vertices are joined by an edge. The **length** of a walk is the number of edges on it. A **path** is a walk without repeated vertices. A **cycle** is a walk of at least three edges without repeated vertices except that the first and last vertex are the same. The terms **path** and **cycle** also refer to the specific graphs that have that structure.

Two vertices are **connected** if there is a walk between them. Being-connected is an equivalence relation; the equivalence classes form the components of the graph. A graph is **connected** if there is only one component.

Here is a graph with three components: a cycle and two trees (one of which is a path).



13.3 Properties of Trees

We discuss next some properties of trees in general.

Lemma 13.1 *A tree is connected and contains no cycle.*

Indeed, this is usually used as the definition of a tree.

Lemma 13.2 *(a) Between any two vertices in a tree there is a unique path.*
(b) Removing any edge disconnects the tree.

Proof. (a) Because a tree is connected, there is at least one path between every pair of vertices. If there were multiple paths between two vertices, then there would be a cycle.

(b) This follows from (a). ♢

In fact the converse of (a) is true: if a graph has the property that between every two vertices there is a unique path, then the graph must be a tree.

How many carbon–carbon bonds are there in an alkane? One can readily see that the number of bonds goes up by 1 each time we add a carbon. This gives us the following result:

Lemma 13.3 *If a tree has n vertices, then it has $n-1$ edges.*

(Note that the above proof is really a lazy form of induction.)

In fact the converse is true. If a graph is connected and has one less edge than vertices, then it must be a tree.

There is also a natural way to **color** the vertices of a tree with two colors. Start by coloring the root with one color, say red. Color its children the other color, say blue. Color their children (the root's grandchildren) with red. And so on, alternating. If we number the generations with the root as 0, then the even generations are red and the odd generations are blue. This has the property that every edge has one red end and one blue end. This is called a **bipartite** coloring.

Exercises

13.1. Determine the number of isomers of pentane and hexane (alkanes with 5 and 6 carbon atoms respectively).

13.2. Prove that a cycle has a bipartite coloring if and only if the number of vertices is even.

13.3. Draw a rooted tree with 5 vertices labeled A, B, C, D, and E such that all of the following conditions hold:
(i) E has exactly two ancestors
(ii) A and C are siblings
(iii) No vertex has exactly one child
(iv) B is neither an ancestor nor a descendant of C
(v) B is not the grandparent of D

13.4. (a) Show that there are exactly two trees on 4 vertices if the vertices are indistinguishable.

(b) How many different trees are there with 4 vertices if the 4 vertices are all distinguishable (say the vertices are labeled `A`, `B`, `C`, `D`)?

(c) How many different rooted trees are there with 4 vertices if the 4 vertices are indistinguishable (and the ordering of children does not matter)?

(d) How many different rooted trees are there with 4 vertices if the 4 vertices are all distinguishable (but the ordering of children does not matter)?

13.5. Consider a simple graph with 100 vertices.

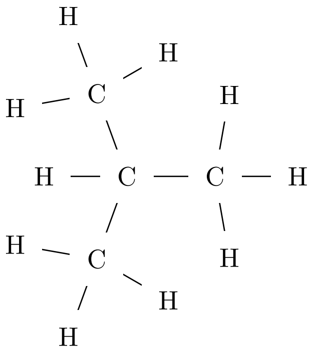
(a) Explain why such a graph has at most $\binom{100}{2}$ edges.

(b) Describe such a graph that has $\binom{99}{2}$ edges but is not connected.

(c) Prove that if such a graph has more than $\binom{99}{2}$ edges then it is connected.

Solutions to Practice Exercises

1.



14 More Graphs: Euler Tours and Hamilton Cycles

14.1 Degrees

The **degree** of a vertex is the number of edges coming out of it. The following is sometimes called the "First Theorem of Graph Theory":

Lemma 14.1 *Suppose the graph has n vertices and a edges. Suppose the degrees of the graph are $d_1, \ldots, d_n$. Then*

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

Proof. This is a double-counting argument: the LHS and RHS count the same quantity, namely "ends of edges". When we sum up the degrees of a graph, we are counting the ends of edges. Each edge has two ends, and so is counted twice. $\diamondsuit$

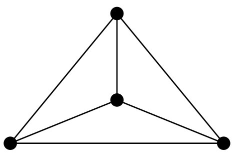
As a consequence we get:

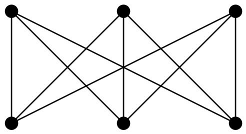
Lemma 14.2 *In any graph, the number of vertices of odd degree is even.*

Proof. We know from the previous result that the sum of the degrees is even. That means that there must be an even number of odd summands. $\diamondsuit$

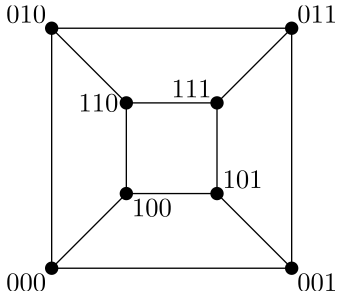
14.2 A Few Good Graphs

The **complete graph** K_n on n vertices is the graph where every pair of vertices are joined by an edge. Thus K_n has $\binom{n}{2}$ edges. The **complete bipartite graph** $K_{r,s}$, for positive integers r and s, has $r+s$ vertices, split into two groups: r vertices on one side, and s vertices on the other. All edges go between the two sides. Here are K_4 and $K_{3,3}$.





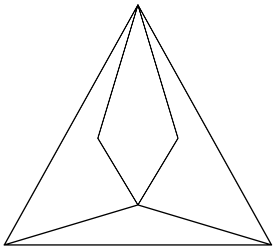
The hypercube is a more interesting graph. The **hypercube** Q_q of dimension q has 2^q vertices. Each vertex corresponds to a bit string (meaning `0`'s and `1`'s) of length q. Two vertices are joined by an edge if their corresponding strings differ in **exactly** one bit. Each vertex therefore has degree q. We can also define Q_q recursively: To form Q_q, take two copies of Q_{q-1} and join each pair of corresponding vertices by an edge. Here is Q_3.



A **subgraph** of a graph G is a graph that contains some of the edges and some of the vertices of the graph G. A subgraph is a **spanning** subgraph if it contains all the vertices of the original graph.

14.3 Eulerian Graphs

For a famous example of a problem, consider the problem of drawing the following picture without lifting your pen and without going over the same line more than once. Try it!



Did you manage to do this? There is a slight trick in that one must start at the bottom of the picture. Why?

A **tour** is a walk in a graph that does not use any edge more than once and ends up where it started. An **Euler tour** is a walk that goes along every edge exactly once, and ends up where one started. This is like the continuous pen drawing, except with the added requirement that one ends at the same place one begins.

Theorem 14.3 *A connected graph has an Euler tour if and only if every vertex has even degree.*

Proof. There are two things to prove. We will prove that if the graph has an Euler tour, then every vertex has even degree. And if every vertex has even degree, then the graph has an Euler tour.

(1) Assume we have an Euler tour. If a vertex has odd degree, then it must be the start or finish of the tour, since if we don't start there, then every time we pass through the vertex we use two of its edges, and so the last time we arrive we are stuck. A graph cannot have exactly one odd vertex (by Lemma 14.2); so it must be that we have no odd vertex.

(2) The second part takes a little bit more work. Define a **tour decomposition** as a collection of tours that use up all the edges of the graph. Assume the graph has every vertex of even degree. Then we claim there is a tour decomposition.

One can construct a tour decomposition in a simple blind fashion: start tracing out a tour until one gets stuck. Since a tour uses an even degree at each vertex, once we remove the first tour, what remains must have even degree throughout. Thus, one can repeat the process, thereby using up all the edges.

But what we want is an Euler tour. This is a tour decomposition consisting of only one tour. So how about this: take the tour decomposition with the minimum number of tours. And suppose there are at least two tours in this decomposition.

Then, because the original graph is connected, there must be somewhere two tours that share a vertex, call it p. We can re-organize things such that p is the start and finish of both tours. But then it is easy to merge the two tours, by continuing on the second after finishing the first. Hence we get a tour decomposition with fewer tours, a contradiction. What was the problem? We supposed that there were two or more tours. In fact, we have an Euler tour. $\Diamond$

The above is a constructive proof: it provides an algorithm for finding an Euler tour. A somewhat more efficient algorithm is to construct the tour directly: start at any vertex, trace along any unused edge and keep on going, except that if there is a **bridge-edge** at a vertex (meaning an edge whose removal would increase the number of components in the remaining graph), you must take it. This algorithm is sometimes attributed to Fleury.

14.4 Hamiltonian Graphs

A **Hamilton cycle** is a cycle that visits every vertex exactly once. That is, a Hamilton cycle is a spanning cycle. Similarly, a **Hamilton path** is a path that visits every vertex exactly once. This idea sounds similar to Euler, but not really. No simple characterization of when a graph has a Hamilton cycle is known. Indeed, it is strongly believed that such a characterization does not exist.

The problem of determining whether a graph has a Hamilton cycle has been proven to be **NP-complete**: while we do not define this concept here, we do point out that there is a \$1 million prize offered for a proof or disproof of the conjecture that none of the NP-complete problems has a polynomial-time algorithm. That is, if you can find an algorithm that runs in at most time proportional to $n^{1000000}$ (where n is the number of vertices) for **all** graphs and is **guaranteed** to determine whether the graph has a Hamilton cycle, then you're a millionaire. Note that there are around $n!$ possible cycles, so checking them all is not going to be anywhere near fast enough.

Lemma 14.4 *(a) The complete graph K_n has a Hamilton cycle for $n \geq 3$.*
(b) The complete bipartite graph $K_{r,s}$ has a Hamilton cycle if and only if $r = s \geq 2$.

We leave the proof of part (b) as an exercise.

The hypercube has a Hamilton cycle. Indeed, Hamilton cycles in the hypercube are called **Gray codes**, and are important in communication. For example, in Q_3 one Gray code is `000, 001, 011, 010, 110, 111, 101, 100, 000`.

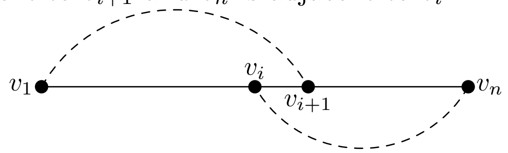
We content ourselves with one sufficient condition and one necessary condition.

Theorem 14.5 *Let G be a graph with n vertices. If every vertex has degree at least $n/2$, then G has a Hamilton cycle.*

Proof. Suppose the theorem is false. That is, there exists a counterexample on n vertices for some n. Then let G be the counterexample on n vertices with the **maximum** number of edges.

Let v_1 and v_n be some pair of vertices not joined by an edge. Since G is a maximum counterexample, it follows that if we add the edge v_1v_n to G, then we have a Hamilton cycle. That is, G has a Hamilton path, say $v_1, v_2, v_3, \ldots, v_n$.

Now, by the hypothesis of the theorem, there are n edges from v_1 and v_n combined to the rest of the graph. This means that, apart from the edges v_1–v_2 and v_{n-1}–v_n, there are $n-2$ edges coming out of v_1 and v_n. For $2 \leq i \leq n-2$, let P_i be the pair of potential edges v_1–v_{i+1} and v_n–v_i. It follows that there must be an i such that both edges in P_i exist; that is, v_1 is adjacent to v_{i+1} and v_n is adjacent to v_i.



By adding in these two edges and deleting the edge v_iv_{i+1}, this gives us a Hamilton cycle, a contradiction. ♢

Theorem 14.6 *If graph G has a Hamilton cycle, then for every set S of vertices, the number of components of $G - S$ is at most $|S|$.*

Proof. Consider the Hamilton cycle C of G. Mark the vertices of S on C. Between each vertex of S we have a piece of C. There are at most $|S|$ pieces of $C - S$, and thus at most $|S|$ components of $G - S$. ♢

The converse of this theorem is false.

Exercises

14.1. Draw all connected graphs with 5 vertices and 5 edges.

14.2. Draw all (simple) graphs with 5 vertices and 7 edges.

14.3. The **degree sequence** of a graph is the sorted sequence of its degrees. Draw a graph with the degree sequence $4, 3, 2, 2, 1, 0$.

14.4. In both the following cases, draw a tree with that degree sequence or prove that it is impossible:

(a) $4, 3, 3, 2, 1, 1, 1, 1, 1$

(b) $4, 3, 3, 2, 1, 1, 1, 1, 1, 1$

14.5. Characterize the degree sequences of trees. That is, state and prove a theorem of the form: There is a tree with degree sequence $d_1, d_2, \ldots, d_n$ if and only if . . .

14.6. Assuming vertices are indistinguishable, draw all (unrooted) trees that have exactly 7 vertices of which exactly 2 vertices have degree exactly 3.

14.7. A **happy tree** is a tree where every vertex has degree 1 or 3.

(a) Draw a happy tree with 10 vertices.

(b) How many different happy trees are there with 10 vertices, assuming vertices are indistinguishable?

(c) Prove that there is no happy tree with 11 vertices.

14.8. Call a tree **orange** if it has 6 vertices and the maximum degree of a vertex is 3.

(a) How many different orange trees are there, assuming vertices are indistinguishable?

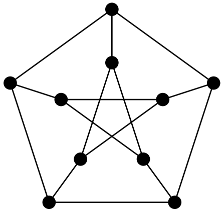
(b) Draw one picture of each orange tree.

14.9. Let T be some fixed tree with 101 vertices.

(a) Show that if every vertex of a graph G has degree at least 100, then we can find a copy of T as a subgraph of G.

(b) Show that the conclusion does not necessary hold if every vertex of G has degree 99.

14.10. Does the following graph have a Hamilton path? A Hamilton cycle?



14.11. Prove Lemma 14.4b.

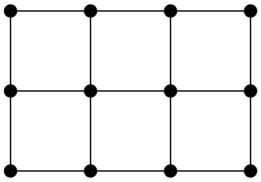
14.12. How many different Hamilton cycles does K_n have? (Note that the answer depends on exactly what one means by two cycles being different; so explain your choice.)

14.13. The Wheel graph W_n is obtained by taking a cycle with n vertices and adding one new vertex that is joined to every vertex in the cycle. Complete the following, with justifications:

(a) W_n has an Euler tour if and only if

(b) W_n has a Hamilton cycle if and only if

14.14. Define the graph G_m as the graph that is a grid of $3m$ vertices arranged in 3 rows and m columns such that each vertex has an edge to the vertices to the left, above, to the right, and below it, if they exist. For example, G_4 is illustrated here.



Complete the following, with justifications:

(a) G_m has an Euler tour if and only if

(b) G_m has a Hamilton cycle if and only if

14.15. A **tournament** is obtained by taking the complete graph K_n and orienting every edge to form a directed graph (where every road is a one-way street).

(a) Show that a tournament always has a directed Hamilton path.

(b) Show that a tournament might not have a directed Hamilton cycle.

14.16. Using the Internet if necessary, look up the term “change ringing”. Explain the connection with Hamilton cycles.

14.17. Using the Internet if necessary, discuss one method to produce Gray codes.

15 Colorings and Planar Graphs

15.1 Bipartite Graphs

We saw already the complete bipartite graph. In general, we say that a graph is **bipartite** if one can partition the vertices into two sets, such that each edge has an end in each set. We saw earlier that trees are bipartite. For, one can pick any vertex as root and partition the vertices into two sets: the even generations and the odd generations. One can also think of the partition as a coloring of the vertices with two colors such that no edge joins two vertices of the same color.

An earlier exercise asked you to prove:

Lemma 15.1 *A cycle is bipartite if and only if it has an even number of vertices.*

The connection between cycles and being bipartite is the following:

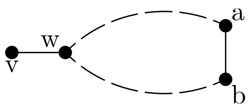
Theorem 15.2 *A connected graph is bipartite if and only if every cycle has even length.*

Proof. There are two things to prove.

(1) If the graph is bipartite, then every subgraph must be bipartite. In particular, every cycle must have even length.

(2) Assume that every cycle has even length. Pick any vertex v. Then for $i \geq 0$, let V_i be the set of vertices at distance i from v. So, for example, V_1 is the neighbors of v, and $V_0 = \{v\}$. Then color red v and every vertex at even distance from v; color the other vertices blue.

Now, we claim that the coloring is a bipartite partition. For, suppose there is an edge joining two vertices red vertices, say a and b. By the definition of distance, a and b are in the same V_i. Then let P_a and P_b be a shortest path from a and b respectively back to v. This path contains one vertex from each V_j for $j < i$. Now, the paths P_a and P_b meet up, at the latest at v. Let w be the first vertex where they meet.



Then the segment a–w of P_a and the segment b–w of P_b have the same length. Thus, adding them and the edge from a to b produces an odd-length cycle, a contradiction. Hence, the coloring is a valid partition. ♢

It follows that there is a simple algorithm to test whether a connected graph is bipartite. Pick any vertex and color it red; color its neighbors blue; color their neighbors red; and so on. If one manages to color all vertices without a conflict, then the graph is bipartite; if one tries to color the same vertex with both colors, then the graph is not bipartite.

15.2 Colorings

A **coloring** of a graph means assigning colors to each vertex such that no edge joins two vertices of the same color. A k**-coloring** means a coloring that uses (at most) k colors. A graph having a 2-coloring is the same thing as being bipartite. The **chromatic number** of a graph, denoted χ, is the minimum number of colors needed for a coloring of the vertices.

Lemma 15.3 *An even cycle has $\chi = 2$.*
An odd cycle has $\chi = 3$.
The complete graph K_n has $\chi = n$.

Proof. Left as an exercise. ♢

One application of chromatic number is the **register allocation problem**. In compiling a program, one would like to use the on-chip registers for as many of the variables as possible. So, construct a graph, where the vertices are the variables, and two vertices are connected by an edge if the corresponding variables can exist simultaneously. A k-coloring of the graph corresponds to an assignment of the variables to k registers.

Let Δ be the maximum degree of a vertex in a graph. It is easy to show that the chromatic number is at most 1 more than the maximum degree:

Lemma 15.4 *If G is a graph with chromatic number χ and maximum degree Δ, then $\chi \leq \Delta + 1$.*

Proof. Use a greedy algorithm. Color the vertices one at a time using the $\Delta + 1$ colors. Each time we color a vertex, we can pick any color not already present amongst its neighbors. That means there are at most Δ forbidden colors. Hence the algorithm cannot get stuck, and creates a coloring with $\Delta + 1$ colors, as required. ♢

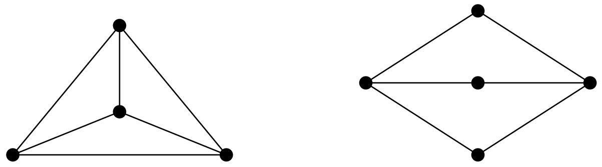
This result can be improved slightly by the following result, whose proof we omit:

Theorem 15.5 [Brooks] *If G is a connected graph that is not complete nor an odd cycle, then $\chi \leq \Delta$.*

It is to be noted that, while testing for bipartiteness is easy, testing whether a graph has a 3-coloring appears to be much, much harder.

15.3 Planar Graphs

A **plane graph** is a graph drawn in the plane such that no pair of lines intersect. The graph divides the plane up into a number of regions called **faces**. Here are plane drawings of K_4 and $K_{2,3}$.



A **planar graph** is one which has a plane drawing. For example, every tree is planar.

Theorem 15.6 *A connected plane graph has one face if and only if it is a tree.*

This is actually much more difficult to prove rigorously than it looks.

Theorem 15.7 Euler's formula. *For connected plane graph with n vertices, a edges, and f faces:*

$$n - a + f = 2$$

Proof. By induction on a. If $a = n - 1$, then G is a tree and we're done. Otherwise $a \geq n$. So there is a cycle containing some edge e. The removal of e merges two faces. Let G' be the resulting plane graph. Then G' has n vertices, $a - 1$ edges and $f - 1$ faces. And so, by the inductive assumption, $n - (a - 1) + (f - 1) = 2$. But the LHS is equal to $n - a + f$. $\diamondsuit$

It follows that:

Theorem 15.8 *For any plane graph on n vertices and a edges, $a \leq 3n - 6$.*

Proof. Let M be the number of edge–face pairs where the edge lies on the boundary of that face. Each edge appears twice: it lies on two boundaries. Each face appears at least three times. So we get $2a = M \geq 3f$. That is, $f \leq 2a/3$. Plug into Euler's formula and do some algebra. $\Diamond$

Consequence: the complete graph K_5 is not planar.

A subdivision of a graph is created by adding some number of new vertices (possibly none) on each edge. A famous result is:

Theorem 15.9 Kuratowski's Theorem. *A graph is planar if and only if it does not contain a subdivision of either K_5 or $K_{3,3}$.*

The most famous theorem in this area is the 4-Color Theorem. This was one of the first major theorems to make extensive use of a computer. It is due to Appel, Haken, and Koch.

Theorem 15.10 Four-Color Theorem. *If G is a planar graph, then $\chi(G) \leq 4$.*

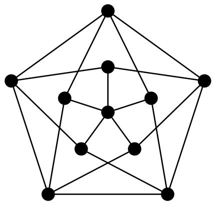
> ▶ **For you to do!** ◀
> *1. Draw a planar graph with 6 vertices and the maximum possible number of edges.*

Exercises

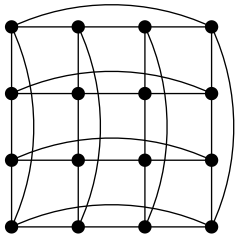
15.1. The wheel W_k is obtained from the cycle on k vertices by adding one new vertex connected to all other vertices. Calculate the chromatic number of a wheel.

15.2. The **prism** of a graph G on n vertices is obtained by taking two separate copies of G and adding n "parallel" edges joining the corresponding vertices. For example, the prism of the hypercube Q_n is Q_{n+1}. State and prove the relationship between the chromatic number of G and the chromatic number of its prism.

15.3. Calculate the chromatic number of the following graph:



15.4. Let T_m be graph constructed as follows. Start with m^2 nodes arranged in a square grid. Then join every node to the node above, below, to the right, and to the left, with wraparound. That is, each node in the top row is joined to the corresponding node in the bottom row (and vice versa); and each node in the leftmost column is joined to the corresponding node in the rightmost column (and vice versa). For example, T_4 is drawn here.



Answer the following, **with justification**.

(a) When does T_m have an Euler tour?

(b) When does T_m have a Hamiltonian cycle?

(c) What is the chromatic number of T_m?

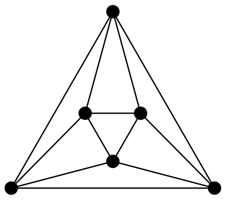
15.5. Show that the maximum number of edges in a bipartite planar graph with n vertices is $2n - 4$.

15.6. Show that $K_{2,m}$ is planar for all m.

15.7. Show that the hypercube Q_4 is not planar.

Solutions to Practice Exercises

1.



16 Introduction to Groups

16.1 Definition

The structure $\mathbb{Z}_n$ we saw earlier is an example of a more general situation. A **group** is a set of elements G together with a single binary operation, call it $\star$, such that it obeys the following rules:

1. G is **closed** under the operation $\star$: that is, for all $a, b \in G$ it holds that $a \star b \in G$;
2. **Associative** law: $a \star (b \star c) = (a \star b) \star c$ for all a, b, c;
3. There is an **identity** e such that for all $a \in G$ we have $a \star e = e \star a = a$; and
4. **Inverses** exist: for all $a \in G$, there is an a^{-1} such that $a \star a^{-1} = a^{-1} \star a = e$.

Note that commutativity is not assumed. Indeed, a group is called **abelian** if it satisfies:

5. Commutative law: $a \star b = b \star a$ for all a, b

In many of our examples, the group operation is addition or multiplication. For example:

- The *positive real numbers* form an abelian group under *multiplication*. Here 1 is the identity, and the inverse of r is $1/r$. Note that all the real numbers does not work, since 0 has no inverse.
- The *integers* form an abelian group under *addition*. Here 0 is the identity, and the inverse of r is $-r$.
- The set of all 2×2 nonsingular *matrices* forms a nonabelian group under matrix *multiplication*. The identity matrix I is the identity, and the inverse of matrix A is A^{-1}.

Notation for the operation: We use the standard symbol if it is a common specific operation, like addition or multiplication. Otherwise, we often use "implicit multiplication" notation: with elements simply written next to each other. The associative law means we can omit brackets completely.

16.2 Basic Facts

Some fundamental properties are the following:

Lemma 16.1
(a) The identity element is unique.
(b) The inverse of an element is unique.
(c) $(a^{-1})^{-1} = a$.
(d) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We show (d). The rest are left as an exercise. To show that something is the inverse, one needs to show that multiplying by it produces the identity. So,

$$(ab) \star (b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = e.$$

Similarly, $(b^{-1}a^{-1})(ab) = e$. $\Diamond$

Note that because we do not assume commutativity, we have to be explicit about whether we are doing the operation on the left or on the right. Nevertheless, $a \star b = a \star c$ implies, multiplying on the left by a^{-1}, that $b = c$. This is often referred to:

Cancellation Law: if $a \star b = a \star c$ then $b = c$; if $b \star a = c \star a$ then $b = c$.

One can produce a **table**, where the (i, j) entry gives the result of the operation applied to the i^{th} entry and the j^{th} entry. Note that each row contains every element exactly once. Why? Every element must be there, since, for any given a and b, the equation $a \star x = b$ has a solution, namely $x = a^{-1} \star b$. By the cancellation law, this solution is unique.

For example, here is the table for a group with four elements $\{e, a, b, c\}$.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

16.3 Modular Groups

Modular arithmetic is where we find two famous abelian groups.

- $\mathbb{Z}_n$. This is the set of integers $\{0, 1, \ldots, n-1\}$ with the operation addition modulo n. The element 0 is the identity, and, apart from 0, $n - a$ is the inverse of a.

- $\mathbb{Z}_n^*$. This is the set of integers in the range 1 up to $n - 1$ that are relatively prime to n, together with multiplication modulo n.

Example 16.1. *Here is the table for* $\mathbb{Z}_{12}^*$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

It takes some checking to see that $\mathbb{Z}_n^*$ is indeed always a group. First, if we multiply two numbers that are relatively prime to n, then the result is still relatively prime to n. So even when we do the mod n part, the result is in $\mathbb{Z}_n^*$. Thus we have closure. The value 1 is, of course, the identity. Recall that the existence of inverses comes from Extended Euclid's algorithm: if $\gcd(a, n) = 1$, then there are s and t such that $as + nt = 1$. Now, if s and n have a common factor, then that is a common factor of $as + nt$, a contradiction. So the inverse s is relatively prime to a, and hence in the set.

16.4 Subgroups

An important concept is a **subgroup**. This is a subset of the elements that contains the identity, and is closed under multiplication and inverses. For example, for the group $\mathbb{Z}$ with addition, the even integers form a subgroup. In general there are always at least two subgroups: the group itself and $\{e\}$. These are called the **trivial** subgroups.

Example 16.2. *The subgroups of* $\mathbb{Z}_n$

The subset of $\mathbb{Z}_n$ consisting of all multiples of a is a subgroup for any a.

EXAMPLE 16.3.

The set of 2×2 matrices with determinant 1 form a subgroup of the set of all nonsingular 2×2 matrices.

A group/subgroup is generated by a set X if it consists of all arbitrary products of elements in X and their inverses. A group that is generated by a single element is called a **cyclic group**.

We use the notation a^n as the notation for n a's multiplied together. Consider the sequence $e, a, a^2, a^3, a^4, \ldots$. If the group is finite, there must come a point in the sequence that we have a repeat. Suppose that first repeat is a^n, and that a^n equals a^m for $m < n$. Then by cancellation $a^{n-m} = e$. So, actually there is no repeat until we reach e. The first positive power of a that equals the identity is called the **order** of a. We also use the term **order** of a group to be the number of elements in the overall group. Thus, the order of an element a is the order of the subgroup generated by a.

Exercises

16.1. (a) Show that the identity element is unique.
(b) Show that the inverse of an element is unique.

16.2. Explain why the following is not a group:

	e	a	b	c
e	e	a	b	c
a	a	a	e	e
b	b	e	b	e
c	c	e	e	c

16.3. Consider the multiplicative group $\mathbb{Z}_{15}^*$

(a) List the elements of the group.

(b) Give the identity element.

(c) Give the inverse of 7.

(d) Give an element other than the identity that is self-inverse.

16.4. Let $q = 2^{100}$. Determine how many elements of $\mathbb{Z}_q$ have order q.

16.5. Show that a nonempty subset S is a subgroup if and only if $a \star b^{-1} \in S$ for all a and b in S.

16.6. (a) Show that the intersection of two subgroups is again a subgroup.
(b) What about union?

16.7. Show that every subgroup of $\mathbb{Z}_n$ is given by the set of multiples of some integer a.

16.8. Show that any subgroup of a cyclic group is itself cyclic.

16.9. (a) Show that if F and H are subgroups of an abelian group, then the set of products $\{\, fh : f \in F, h \in H \,\}$ is also a subgroup.
(b) Explain where in your proof you used the fact that the group is abelian.

16.10. Consider the set $\mathbb{Z}[\sqrt{2}] = \{\, a + b\sqrt{2} : a, b \in \mathbb{Z} \,\}$. Show that $\mathbb{Z}[\sqrt{2}]$ is a group under addition.

16.11. Fix some set X. Let G be the set of all subsets of X. For $A, B \in G$, define $A \triangle B$ to be the set of all elements that are in exactly one of A or B; that is, $A \triangle B = (A - B) \cup (B - A)$. Show that G is an abelian group under $\triangle$.

17 More Groups, Lagrange's Theorem and Direct Products

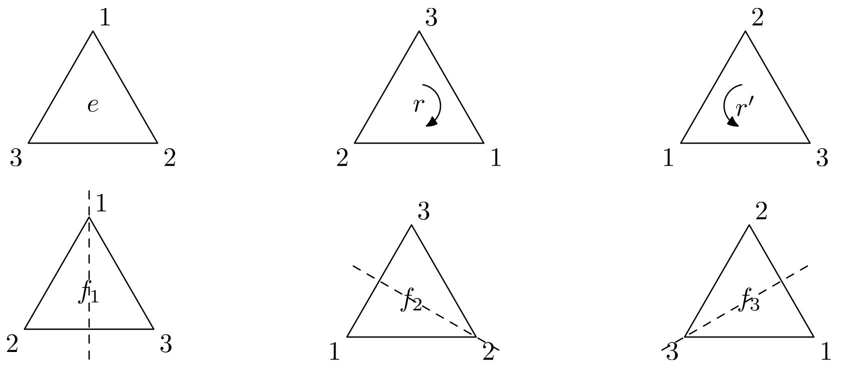
We consider several ways to produce groups.

17.1 The Dihedral Group

The **dihedral group** D_n is a nonabelian group. This is the set of "symmetries" of a regular n-gon: the motions that leave the n-gon looking unchanged. One can rotate the polygon $360/n$ degrees, or indeed any multiple thereof. One can also think of reflection around various axes. Specifically, the dihedral group has $2n$ elements. There are $n-1$ **rotations** and n flips. For motions m_1 and m_2, we define $m_1 \medwhitestar m_2$ to be the motion obtained by m_1 followed by m_2.

Example 17.1. *Consider D_3.*

This is the symmetry group of an equilateral triangle. Say r is the rotation 120 degrees clockwise, r' the rotation 120 degrees counterclockwise, and f_i the flip around an axis through the center and corner labeled i. Then we get the pictures and table.



	e	r	r'	f_1	f_2	f_3
e	e	r	r'	f_1	f_2	f_3
r	r	r'	e	f_2	f_3	f_1
r'	r'	e	r	f_3	f_1	f_2
f_1	f_1	f_3	f_2	e	r'	r
f_2	f_2	f_1	f_3	r	e	r'
f_3	f_3	f_2	f_1	r'	r	e

In general, in D_n a flip is its own inverse. The inverse of a rotation is another rotation. Other group properties can be checked.

17.2 Lagrange's Theorem

There is a famous result about the relationship between finite groups and subgroups:

Theorem 17.1 *Lagrange's Theorem. The order of a subgroup divides the order of the group.*

We will attempt a proof of Lagrange's Theorem in a moment. A special case is that, if the group is finite, then the order of an element divides the order of the group. One consequence of this is **Fermat's Little Theorem**. This follows from Lagrange's theorem, because the order of element a is a divisor of the order of $\mathbb{Z}_p^*$, which is $p-1$.

17.3 Coset Groups and a Proof of Lagrange's Theorem

We show how to partition a group based on a subgroup of a group.

Let G be a group. For a subgroup H and $a \in G$, the **left coset** aH is the set of elements $\{ ah : h \in H \}$. That is, take everything in H and multiply on the left by a. (Right cosets are defined similarly.)

Note that the elements of aH have to be distinct (by the cancellation law). So, H has the same size as any left coset. Indeed, in particular each coset has the same size. Now, the key observation (which basically says being in the same coset is an equivalence relation):

Lemma 17.2 *If two cosets of H intersect, then they are equal.*

Proof. Suppose cosets aH and bH intersect. That is, $ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then consider any element of aH, say ah. Then $ah = bh_2h_1^{-1}h$; since $h_2h_1^{-1}h \in H$, it follows that $ah \in bH$. Similarly, every element of bH is in aH. Thus the cosets are identical. $\Diamond$

It follows that the left cosets form a partition of G, and each coset has the same size. So:

> *the order of group G is the order of subgroup H times the number of distinct cosets of H.*

From this, Lagrange's theorem follows.

17.4 Direct Sums

Let G and H be groups. The **direct sum** (or direct product) of G and H is a new group written $G \times H$. It is formed by taking all ordered pairs, one element from G and one element of H, with vector operation. That is,

$$(a, b) \star (c, d) = (a \star_G c,\ b \star_H d).$$

It can be checked that the result is a group. The identity is (e_G, e_H). The inverse of (a, b) is (a^{-1}, b^{-1}).

Note that the direct sum of abelian groups is itself abelian.

EXAMPLE 17.2. *Consider* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

This contains $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$. Its table is:

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

17.5 Group Isomorphism

What makes two groups the same? We say that groups G and H are **isomorphic** if there is a bijective mapping $f\colon G \to H$, such that $f(a \star_G b) = f(a) \star_H f(b)$. By **bijective**, we mean that every element of G is paired with a unique element of H and vice versa. The mapping f is called an **isomorphism**.

EXAMPLE 17.3. $\mathbb{Z}_6^*$ *is isomorphic to* $\mathbb{Z}_2$.

For, the former has set $\{1, 5\}$ and the latter has set $\{0, 1\}$. If we map $1 \mapsto 0$ and $5 \mapsto 1$, then the mapping is bijective, and the operation is preserved (the table looks the same).

Indeed, it is not hard to show that all groups with 2 elements are isomorphic.

EXAMPLE 17.4. $\mathbb{Z}_2 \times \mathbb{Z}_3$ *is isomorphic to* $\mathbb{Z}_6$.

The bijection is $(a, b) \to (3a + 2b) \bmod 6$.

Example 17.5. *$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$.*

(Think how the tables compare.)

Note:

- To show two groups are isomorphic, find a bijection.
- To show two groups are not isomorphic, find a property that one of them has that the other one doesn't.

There is a general theorem about such products:

Theorem 17.3 *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to the group $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.*

We leave the proof as an exercise.

While nonabelian groups are very rich and varied, in some sense we know exactly the range of abelian groups. Using a lot more work, it can be shown that:

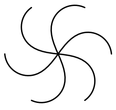
Theorem 17.4 *Every finite abelian group is isomorphic to the direct sum of cyclic groups.*

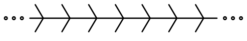
Exercises

17.1. Determine the group of symmetries of the following shapes:

(a) The letter: S

(b) The plus sign: +

(c) A flower 

(d) This shape is infinite: 

17.2. Prove that two cosets aH and bH are equal if and only if $b^{-1}a \in H$.

17.3. Consider the group of 2×2 matrices with nonzero determinant.

(a) Give an element of order 2.

(b) Give a nontrivial/proper subgroup.

17.4. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_5$.

(a) What is the order of the group?

(b) What is the identity?

(c) List all elements of order 5.

17.5. Consider the complex numbers $\{1, -1, i, -i\}$ with operation multiplication. What group is this isomorphic to?

17.6. Prove that, if G has even order, then it must have an element of order 2.

17.7. Show that if p is a prime, then all groups of order p are cyclic and indeed isomorphic.

17.8. Suppose groups G and H each have order 100 and each contain an element of order 100. Prove that G and H are isomorphic.

17.9. Prove that every group of order 15 is cyclic.

17.10. Consider the following table for a group.

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	a	e	g	h	f	d
c	c	b	e	a	h	g	d	f
d	d	f	h	g	a	e	b	c
f	f	d	g	h	e	a	c	b
g	g	h	d	f	c	b	a	e
h	h	g	f	d	b	c	e	a

(a) What is the identity?

(b) Give an element of order 4.

(c) Is the group abelian? (Justify your answer.)

(d) Explain why we know this is not the dihedral group D_4.

17.11. (a) Determine all the subgroups of the dihedral group D_4.
(b) Determine all the subgroups of the dihedral group D_5.

17.12. Determine all the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

17.13. (a) Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is not isomorphic to $\mathbb{Z}_{mn}$ if m and n are not relatively prime.

(b) Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if m and n are relatively prime.

17.14. Let group $G = \mathbb{Z}_{9409} \times \mathbb{Z}_{97}$. Note that 97 is prime and that $9409 = 97^2$.

(a) What is the identity element in G?

(b) How many elements of order 97 does G have? Justify your answer.

(c) How many elements of order 98 does G have? Justify your answer.

17.15. Consider any group where every element except the identity has order 2. Prove that the group must be abelian. (Hint: start with $a \star b \star a \star b$.)

18 An Introduction to Codes

This chapter assumes the reader is familiar with the basics of linear algebra.

Mathematics uses the term code to mean something used to send data where the data is recoverable even if the message is somewhat corrupted. This is different to encryption, where the goal is to send data that is private.

18.1 Two Simple Codes

We assume the data is given as a binary string.

Example 18.1. *Check-bits*

The **check-sum** of a string is the sum of all the bits, modulo 2. For example, if the data is `01101`, then the check-sum is `1`. The message sent is the data with the check-sum appended.

The claim is that: *the receiver is able to detect if exactly one of the bits is changed in transmission.* For, the check-bit is `0` if and only if the original data contains an **even** number of `1`'s. So if exactly one of the data bits is changed, the the check-sum is wrong. Similarly a change in the check-sum is also detectable. But note that there is absolutely no information as to where the error was. And if two of the bits are changed then the error is undetectable.

Check sums are used in many other places. For example, the ISBN number of a book has last digit a check-sum.

Example 18.2. *Repetition Code*

In a repetition code, every bit is sent multiple times. Say every bit is sent three times. This code has the power to detect and correct a single bit error. Indeed, this code can handle multiple errors, as long as they don't occur twice in the same triple. However, it is inefficient, as what is sent is three times as long as the original data.

18.2 Binary Linear Codes

Both of the above are examples of linear codes. In a **binary linear code**, each sent bit is a linear combination of the data bits. That is, we think of the data d as a binary vector, and the code e that is sent is given by

$$e = d\,M$$

where matrix M, called the **generator matrix**. Arithmetic is modulo 2 (or equivalently, in the group $\mathbb{Z}_2$).

Here are the generator matrices for the above two codes, in the case that d has three bits:

$$C_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad D_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

18.3 Some Theory

For two vectors of the same length, their **Hamming distance** is the number of places the corresponding entries are different.

Given a code, an important collection is the set of all vectors generated (aka the range of the linear transform or the row-space of the generator matrix). The **distance** of a code is the minimum Hamming distance between any two vectors in it.

Theorem 18.1 *(a) A code can detect k errors if and only if its distance is at least $k+1$. (b) A code can correct k errors if and only if its distance is at least $2k+1$.*

Proof. If there are at most k errors, then the Hamming distance between the sent vector and the received vector is at most k. Thus the received vector can be another possible transmission vector if and only if the distance of the code is k or less.

Further, to correct the errors, there must be a unique possible sent vector that is closest to the received vector. So any vector can be Hamming distance at most k away from one sendable vector. If the distance of the code is at least $2k+1$, then this will be true. If the distance of the code is $2k$, say between vectors e_1 and e_2, then any vector "half-way" between e_1 and e_2 cannot be corrected without the possibility of error. $\diamondsuit$

18.4 Hamming Codes

Now, what one would like in a code is a code that (a) is efficient (the sent message is not much longer than the original) and (b) that is easy to decode (if the code has the property that one can correct some number of errors, then these corrections can be done quickly).

One idea is the **Hamming code**. There are 4 data bits and 3 check bits. The 1st check bit is for the 1,2,4 data bits, the 2nd check bit is for the 1,3,4 data bits, and the 3rd check bit is for 2,3,4 data bits. For example, suppose the data is `1101`. Then the first check bit is `1`, the second is `0`, and the third is `0`.

Note that each data bit affects two or more of the check bits. This means that if one of the data bits is changed, at least two of the check-bits are flipped. That is, the distance of this code is at least 3. So by the above theorem, one can correct one error.

But the neat idea of Hamming was how to do the decoding quickly. Specifically, Hamming placed the three check bits in positions 1, 2 and 4 of the resultant code. That is, the generator matrix is:

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

For example, suppose the data is `1101`. Then the sent message is `1010101`.

To decode, take the received message and verify the check bits. Then:

> Construct a number p as follows. Start with $p = 0$. If the first check bit is wrong, add 1 to p; if the second check bit is wrong, add 2 to p; and if the third check bit is wrong, add 4 to p. The final value of p says which bit in the received message was flipped!

For example, suppose that string `1010001` is received. Then the (alleged) data is `1001` and the 1st and 3rd check bits are wrong. That is $p = 1 + 4 = 5$. And, hey presto, that is correct.

Of course, the real question is where did this come from and why does it work. Well, note first that when we write the message as `ccDcDDD`, the positions of the check bits are powers of 2. Further, the first check bit is dependent on all positions which, written in binary, have a 1 in the last column, namely $1, 3, 5, 7$; the second check bit is dependent on all positions which, written in binary, have a 1 in the middle column, namely $2, 3, 6, 7$; and the third check bit is dependent on all positions which, written in binary, have a 1 in the first column, namely $4, 5, 6, 7$.

In general, one can build a Hamming code with c check bits and $2^c - c - 1$ data bits.

18.5 Reed–Muller Codes

We specify a specific family of Reed-Muller codes by the set of strings in it. This is an inductive definition.

> Start with $R_1 = \{\texttt{0}, \texttt{1}\}$. The set R_{m+1} is obtained from the set R_m by taking every string w in R_i and writing down both ww and $w\overline{w}$, where $\overline{w}$ means string w with all the bits flipped.

For example, R_2 is all 2-bit strings. The strings in R_m have length 2^{m-1} and there are 2^m of them. (Check!)

The key claim is that: *the distance of R_m is at least 2^{m-1}.* The proof is by induction. True for the base case $m = 1$. Assume true for R_{m-1}. Note that the code is *closed* under flipping all bits; that is, if w is a string in R_{m-1} then so if $\overline{w}$. So when we write down ww or $w\overline{w}$, the first half is by the IH distance at least 2^{m-2} from all other first halves. By the induction hypothesis, the second half is also distance at least 2^{m-2} from all other second halves, unless that half is exactly the same as some other second half. But in that case we are dealing with $\overline{w}\,\overline{w}$. Thus two new code-strings are are at least distance 2^{m-1} from each other.

It might not be obvious from the above that we can represent as a generator matrix. But it is possible. And again there is a nice decoding algorithm. And by starting with a different set, one can obtain codes with other properties.

Exercises

18.1. We saw above the Hamming code with 3 check bits. Explain what the Hamming code with 2 check bits looks like.

18.2. For the Hamming code with 4 check bits, there are 11 data bits. Determine the 4 check bits for
(a) the data `00000000000`
(b) the data `11111111111`
(c) the data `10101010101`

18.3. For the general Hamming code with k check bits, show that the distance is exactly 3.

18.4. Show that the distance of the Reed–Muller code R_m is exactly 2^{m-1}.

18.5. Consider the Reed–Muller code R_3.
(a) List all strings in R_3.
(b) Provide a suitable generator matrix.

18.6. (a) Consider a code with distance d with d odd. Show that if one appends a parity bit to every string, then the new code has distance $d + 1$.
(b) Give an example that shows that part (a) is not necessarily true if d is even.

References

- *Finite Mathematics*, S.C. Althoen and R.J. Bumcrot, Norton, 1978.
- *An Introduction to Cryptography*, Course-notes: University of Natal, G.Barbour, 1998.
- *Fundamentals of Algorithmics*, G.Brassard and P.Bratley, Prentice-Hall, 1996.
- *Graphs & Digraphs* (various editions), G. Chartrand and L. Lesniak.
- *Introduction to Algorithms*, T.H.Cormen, C.E.Leiserson, and R.L.Rivest, MIT Press, 1990.
- *A First Course in Abstract Algebra*, J.B. Fraleigh, Addison-Wesley, 1982.
- *Pearls in Graph Theory*, N. Hartsfield and G. Ringel, Academic Press, 1990.
- *Cryptography: Theory and practice*, D.R.Stinson, CRC Press, 1995.
- *Data Structures and Problem Solving in Java* (3rd ed), M.A. Weiss, Addison-Wesley, 2005.
- *Introduction to Graph Theory*, D. West, Prentice-Hall, 1996.
- wikipedia.org