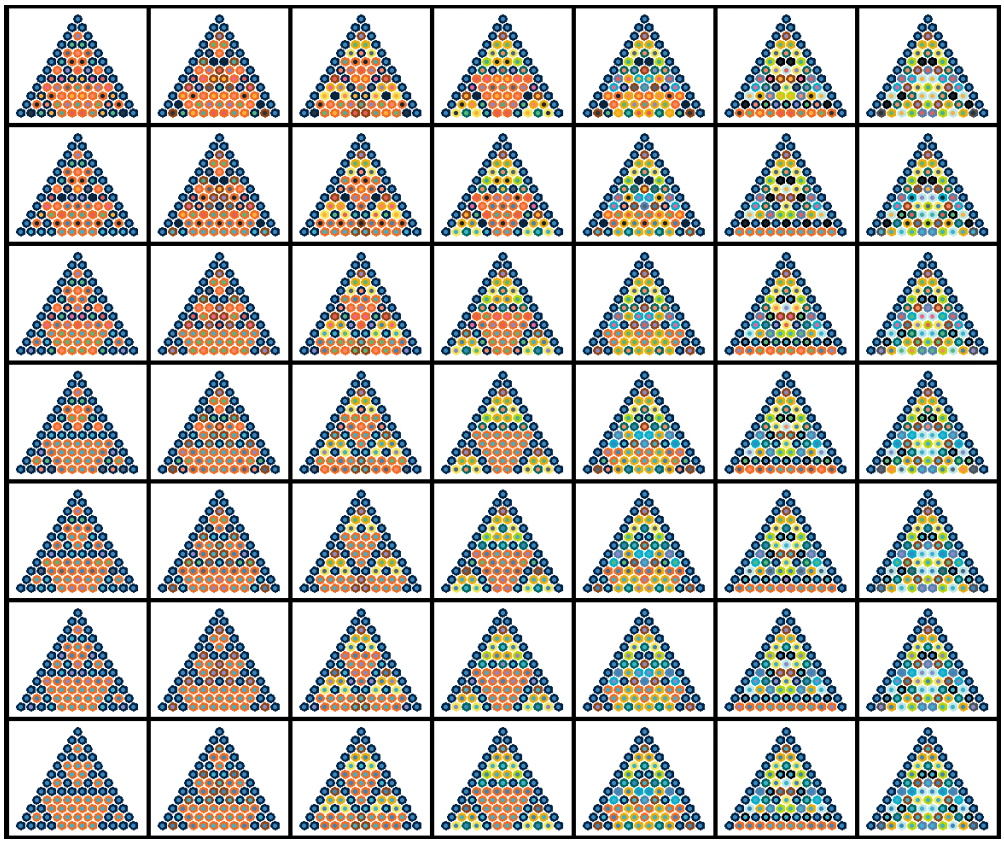
An Active Introduction to Discrete Mathematics



Charles A. Cusack
cusack@hope.edu

Version 4.0
June 10, 2025

History (2025) Created this book from "An Active Introduction to Discrete Mathematics and Algorithms," Version 3.5. This is a subset of that book, with the chapters on algorithms and algorithm analysis removed, examples related to algorithms and algorithm analysis greatly reduced, and other edits here and there.

About the cover
Pascal's Triangles colored differently to show structural properties relating to factors of the binomial coefficients that make up the triangle. Created by Charles Cusack. For more of Dr. Cusack's digital art, go to https://cusack.hope.edu/Art/

Contents

Preface

This book is a subset of the material from "An Active Introduction to Discrete Mathematics and Algorithms," Version 3.5 (https://cusack.hope.edu/Notes/Notes/Books/AIDMA/AIDMA.3.5.pdf). If you want a textbook suitable for use primarily by computer science students, especially those who have already had programming and data structures courses, that version of the book might be a better choice.

The majority of material related to algorithms has been removed from this book (Thus the title change), and this version of the book is now suitable for use with secondary mathematics education students (specifically designed to meet certain requirements in the state of Michigan), computer science students, and general education students. No prerequisites are assumed in this version of the book.[1]

The content is arranged to allow a course to focus more or less on proof writing. For instance, Sections 3.1.3, 3.3.2, 5.1.3, and 5.1.4 separate proofs involving sets, functions, and asymptotic notation so they can be skipped if desired.

Since the textbook has gone through some major changes, I definitely appreciate any feedback, positive or negative (preferably constructive, though!), so that I can continue improving it. If you see things that seem out of place, topics that you think should be there, notice other problems, or have suggestions, please let me know.

Charles A. Cusack
Professor of Computer Science
Hope College
cusack@hope.edu
June, 2025

[1]For the most part, anyway. There is a bit of calculus assumed in one section related to proofs of asymptotic notation using limits, but that section can be skipped.

Note to Instructors

Here is an anecdote on how I personally use the book that you might find helpful. The `TL;DR` version: I have my students answers all exercises and reading questions before class and their unanswered questions are where each class period begins, and often lingers. I rarely (never?) lecture through material when I use this textbook. Students seem to like it and they are learning.

At the beginning of each semester, I have each student share a Google Doc with me called *Smith RQ*, where they replace *Smith* with their last name. Every time I assign reading from the textbook, I tell them to write answers to all of the exercises in the assigned sections of the book (my students buy a printed copy of the book), and to put their answers to all of the reading questions into their Google Doc, placing the most recent answers at the top of the document (to make it quicker for me to find).[2] I quickly go through their documents to make sure they have filled out answers to the reading questions for the day, giving them 0-4 points depending on how they did.[3] For sake of time, I only grade them based on attempt, not content.[4] If they attempted to answer all of the questions (including answers such as "I'm not sure how to do this one"), they get 4 points. For half, they get 2. If they skip it, a big fat zero! You get the idea. When I have time, I do this before class so I can also take a brief look at some of the answers to get a sense of how the class is doing on the material.[5]

At the beginning of class, I pick a random[6] page from the reading that has exercises on it and ask all of them to show me their book. If they attempted to answer all of the questions on the page (both displayed pages), they get 4 points. If they tried some of them, they get 2 or 3. If they forgot to do it, they get 0.

I count these attempts as part of their grade so that they have motivation to do it, but since the grades *should* be fairly high on these, I do not want it to count for too much. I call this category *Activities* or *Preparation*, and it is often worth 5-15% of their final grade. My exams and homework are generally sufficiently difficult to compensate for the fact that many of the students will have really high scores in this category.

If one had access to a grader, a nice slight modification would be to pick a handful of questions to grade for content, and the rest for completion. That can work for both the exercises (they can put select answers in their Google Doc, for instance) and the reading questions. On the other hand, since answers to the exercises and reading questions are available in the book, I am not sure that much is gained by grading these for content.

I spend the next part of class, and often the entire class, focusing on answering questions from the exercises and reading questions that stumped them. I rarely lecture through material in this

[2] This could be done the old-fashioned way on pencil and paper, or by having them submit it via a CMS, but using a Google Doc means that the deadline is flexible and they do not have to repeatedly turn their answers in since they just prepend them to the document they have already shared with me.

[3] Why 0-4? Since 4 is even, they can get half credit. And 5 categories seems like a good number. The way I usually assign grades, 0-2 would also work since very rarely do I give someone 1 or 3 points. But you do you.

[4] I think it is very important that students know when they are being graded on effort instead of outcome since I never want them to get a sense that they did something correct based on the fact that I did not mark it down. I make it very clear to my students that it is their responsibility to grade their own work and they need to ask questions if they are uncertain about any of their answers.

[5] When my schedule allows me a free hour before class, I have the reading questions due an hour before class. Other semester I have them due at midnight the night before or mid-morning to allow me time to look at them before class.

[6] By "random" I really mean a page that is usually in the second half of the reading and has multiple questions on it.

course. I expect that they will learn the mundane parts (e.g. basic definitions) through reading, and we can focus our time during class on the more complicated concepts and applying the ideas.

I have used this technique for over a decade and it seems to work well. In addition, most of my students appreciate the way the textbook is written and how I use it since it forces them to do the reading (that they otherwise would skip doing) and they get useful feedback along the way. On the other hand, they do mention that it is a lot of work—reading, answering exercises, and answering reading questions takes a lot longer than just skimming, which is what many of them would likely do otherwise. But in the end, they definitely seem to fall on the side of liking this approach.

Charles A. Cusack
June, 2025

Note to Students

As the title of the book indicates, this is not a book that is just to be read. It was written so that the reader interacts with the material. If you attempt to just read what is written and take no part in the exercises that are embedded throughout, you will likely get very little out of it. Learning needs to be active, not passive. The more active you are as you 'read' the book, the more you will get out of it. That will translate to better learning. And it will also translate to a higher grade. So whether you are motivated by learning (which is my hope) or merely by getting a certain grade, your path will be the same–use this book as described below.

The content is presented in the following manner. First, concepts and definitions are given–generally one at a time. Then one or more examples that illustrate the concept/definition will be given. After that you will find one or more exercises of various kinds. This is where this book differs from most. Instead of piling on more examples that you merely read and *think* you understand, you will be asked to solve some for yourself so that you can be more confident that you really *do* understand.

Some of the exercises are just called *Exercises*. They are very similar to the examples, except that you have to provide the solution. There are also *Fill in the details* which provide part of the solution, but ask you to provide some of the details. The point of these is to help you think about some of the finer details that you might otherwise miss. There are also *Questions* of various kinds that get you thinking about the concepts. Finally, there are *Evaluate* exercises. These ask you to look at solutions written by others and determine whether or not they are correct. More precisely, your goal is to try to find as many errors in the solutions as you can. Usually there will be one or more errors in each solution, but occasionally a correct solution will be given, so pay careful attention to every detail. The point of these exercises is to help you see mistakes before you make them. Many of these exercises are based on solutions from previous students, so they often represent the common mistakes students make. Hopefully if you see someone else make these mistakes, you will be less likely to make them yourself.

The point of the exercises is to get you thinking about and interacting with the material. As you encounter these, you should write your solution in the space provided. After you have written your solution, you should check your answer with the solution provided in the back of the book. You will get the most out of them if you first do your best to give a complete solution on your own, and then *always* check your solution with the one provided to make sure you did it correctly. If yours is significantly different, make sure you determine whether or not the differences are just a matter of choice or if there is something wrong with your solution.

If you get stuck on an exercise, you should re-read the previous material (definitions, examples, etc.) and see if that helps. Then give it a little more thought. For *Fill in the details* questions, sometimes reading what is past a blank will help you figure out what to put there. If you get *really* stuck on an exercise, look up the solution and make sure you fully understand it. But don't jump to the solution too quickly or too often without giving an honest attempt at solving the exercise yourself. When you do end up looking up a solution, you should always try to rewrite it in the space provided *in your own words*. You should not just copy it word for word. You won't learn as much if you do that. Instead, do your best to fully understand the solution. Then, without looking at the solution, try to re-solve the problem and write your solution in the space provided. Then check the solution again to make sure you got it right.

It is highly recommended that you act as your own grader when you check your solutions. If your solution is correct, put a big check mark in the margin. If there are just a few errors, use a

different colored writing utensil to mark and fix your errors. If your solution is way off, cross it out (just put a big 'X' through it) and write out your second attempt, using a separate sheet of paper if necessary. If you couldn't get very far without reading the solution, you should somehow indicate that. So that you can track your errors, I highly recommend crossing out incorrect solutions (or portions of solutions) instead of erasing them. Doing this will also allow you to look back and determine how well you did as you were working through each chapter. It may also help you determine how to spend your time as you study for exams.

This whole process will help you become better at evaluating your own work. This is important because you should be confident in your answers, but only when they are correct. Grading yourself will help you gain confidence when you are correct and help you quickly realize when you are not correct so that you do not become confident about the wrong things. Another reason that grading your solutions is important is so that when you go back to re-read any portion of the book, you will know whether or not what you wrote was correct.

It is important that you read the solutions to the exercises after you attempt them, even if you think your solution is correct. The solutions often provide further insight into the material and should be regarded as part of any reading assignment given.

Make sure you read carefully. When you come upon an *Evaluate* exercise, do not mistake it for an example. Doing so might lead you down the wrong path. Never consider the content of an *Evaluate* exercise to be correct unless you have verified with the solution that it is really correct. To be safe, when re-reading, always assume that the *Evaluate* exercises are incorrect, and never use them as a model for your own problem solving. To help you, we have tried to differentiate these from other example and exercise types by using a different font.

There is an expectation that you are able to solve every exercise on your own. (Note that I am talking about the exercises embedded into the chapters, not the homework problems at the end of each chapter.) If there are exercises that you are unable to complete, you need to get them cleared up immediately. This might mean asking about them in class, going to see the professor or a teaching assistant, and/or going to a help center/tutor. Whatever it takes, make sure you have a clear understanding of how to solve all of them.

Every chapter ends with two sections called *Reading Comprehension Questions* and *Problems*. The *Problems* sections are exactly what they sound like–a list of problems suitable for working on in class or given as homework assignments.

All of the *Reading Comprehension Questions* should be attempted after you have finished reading each section (including completing all of the exercises). They are sort of the final check of your comprehension of the material before you move on to solving homework problems. Although some of these questions are similar to the exercises in the sections, others are more conceptual in nature. The majority of them are not meant to be difficult, but rather to test whether you really understand the material from the section as whole. These can be used as a starting point for class discussion, so be sure to ask about those that you have trouble completing and/or are unsure about.

Space is not given in the book for solutions to the *Reading Comprehension Questions*, so write your answers on paper or use a Google Doc or other typesetting software to record your solutions. (In my classes I have students share a Google Doc with me in which they place their answers to these questions, adding the most recent answers at the top of the document to make it easier to find their recent answers. When questions can't easily be done in a Google Doc, they write their solution on paper, scan or take a picture of it, and include the picture in their Google Doc.)

Solutions to the *Reading Comprehension Questions* are available in the back of the book. As with the exercises throughout the book, it is highly recommended that you check your answers and grade your own work, crossing out your solution when you were incorrect (instead of erasing/deleting it) and replacing it with the correct solution.

Chapter 1: Logic

1.1 Propositional Logic

1.1.1 Basic Definitions

Definition 1.1. *A* **boolean proposition** *(or simply* **proposition***) is a statement which is either* **true** *or* **false** *(sometimes abbreviated as* **T** *or* **F***). We call this the* **truth value** *of the proposition.*

Whether the statement is *obviously* true or false does not enter into the definition. One only needs to know that its certainty can be established.

Example 1.2. The following are propositions and their truth values, if known:

(a) $7^2 = 49$. (**true**)

(b) $5 > 6$. (**false**)

(c) If p is a prime then p is odd. (**false**)

(d) There exists infinitely many primes which are the sum of a square and 1. (unknown)

(e) Dr. Cusack is the Pope. (**false**)

(f) Every even integer greater than 6 is the sum of two distinct primes. (unknown)

Note: *Next you will see the first of many* **Exercises**. *These give you an opportunity to solve a problem from start to finish and then check your answer with the solution provided. It is important that you try each of these on your own before looking at the solution. You will not get as much out of the book if you skip these or jump straight to the answer without trying them yourself.*

★**Exercise 1.3.** Give the truth value of each of the following statements.

(a) _____ $0 = 1$.

(b) _____ 17 is an integer.

(c) _____ In 1999, it was possible to buy a red Swingline stapler.

Note: *Did you notice the ⋆ in the heading of the previous example? This indicates that a solution is provided. If you are reading the PDF file, clicking on the ⋆ will take you to the solution. Clicking on the number in the solution will take you back.*

If you are reading the PDF, go to the back of the book to find the solutions.

Example 1.4. The following are not propositions, since it is impossible to assign a **true** or **false** value to them.

(a) Whenever I shampoo my camel.

(b) Sit on a potato pan, Otis!

(c) What I am is what I am, are you what you are or what?

(d) $x = x + 1$.

(e) This sentence is false.

★**Exercise 1.5.** For each of the following statements, state whether it is true, false, or not a proposition.

(a) _____ i can has cheezburger?

(b) _____ "Psych" was one of the best shows on TV when it was on the air.

(c) _____ I know, right?

(d) _____ This is a proposition.

(e) _____ This is not a proposition.

1.1.2 Compound Propositions

Definition 1.6. *A* **logical operator** *is used to combine one or more propositions to form a new one. A proposition formed in this way is called a* **compound proposition***. We call the propositions used to form a compound proposition* **variables** *for reasons that should become evident shortly.*

Next we will discuss the most common logical operators. Because one of the applications of logic we will be concerned about is algorithms and programming, when we introduce notation we will also mention equivalent notations used in several common programming languages. For each of the following definitions, assume p and q are propositions.

Definition 1.7. *The* **negation** *(or* **NOT***) of p, denoted by* $\neg \boldsymbol{p}$ *is the proposition "***it is not the case that** $\boldsymbol{p}$*". $\neg p$ is true when p is false, and vice-versa. Other notations include $\overline{p}$, $\sim p$, and $!p$. Many programming languages use the last one.*

Example 1.8. If p is "$x < 0$", then $\neg p$ is "It is not the case that $x < 0$," or "$x \geq 0$."

Note: *The next example is the first of many* **Fill in the details** *exercises in which* **you** *need to supply some of the details. After you have filled in the blanks, compare your answers with the solutions. The answers are often given with semicolons (;) separating the blanks.*

★**Fill in the details 1.9.** Let p be the proposition "I am learning discrete mathematics."

Then $\neg p$ is the proposition _____.

The truth value of $\neg p$ is _____.

Definition 1.10. *The* **conjunction** *(or* **AND***) of p and q, denoted by* $\boldsymbol{p \wedge q}$*, is the proposition "***p and q***". The conjunction of* **p** *and* **q** *is true when* **p** *and* **q** *are both true and false otherwise. Many programming languages use* `&&` *for conjunction.*

Example 1.11. Let p be the proposition "$x > 0$" and q be the proposition "$x < 10$." Then $p \wedge q$ is the proposition "$x > 0$ and $x < 10$," or "$0 < x < 10$."

Example 1.12. Let p be the proposition "$x < 0$" and q be the proposition "$x > 10$." Then $p \wedge q$ is the proposition "$x < 0$ and $x > 10$."

Notice that $p \wedge q$ is always false since if $x < 0$, clearly $x \not> 10$. But don't confuse the *proposition* with its *truth value*. When you see the statement '$p \wedge q$ is "$x < 0$ and $x > 10$"' and '$p \wedge q$ is false,' these are saying two different things. The first one is telling us what the proposition is. The second one is telling us its truth value. '$p \wedge q$ is false' is just a shorthand for saying '$p \wedge q$ has truth value false.'

★**Fill in the details 1.13.** If p is the proposition "I like cake," and q is the proposition "I like ice cream," then $p \wedge q$ is the proposition _____.

Definition 1.14. *The* **disjunction** *(or* **OR***) of p and q, denoted by* $\boldsymbol{p \vee q}$*, is the proposition "***p or q***". The disjunction of* **p** *and* **q** *is false when both* **p** *and* **q** *are false and true otherwise. Put another way, if* **p** *is true,* **q** *is true, or both are true, the disjunction is true. Many programming languages use* `||` *for disjunction.*

Example 1.15. Let p be the proposition "$x < 5$" and q be the proposition "$x > 15$." Then $p \vee q$ is the proposition "$x < 5$ or $x > 15$." In a Java/C/C++ program, it would be "`x<5 || x>15`."

★**Fill in the details 1.16.** Let p be the proposition "$x > 0$" and q be the proposition "$x < 10$." Then $p \vee q$ is the proposition _____.

Notice that $p \vee q$ is always _____ since it is _____ if $x > 0$, and if $x \not> 0$, then clearly _____, so it is _____ then as well.

★**Exercise 1.17.** Let p be "Jill is tall," and q be "Jill is smart." Express each of the following propositions in English.

(a) $\neg p$ is _____

(b) $p \vee q$ is _____

(c) $p \wedge q$ is _____

(d) $p \wedge \neg q$ is _____

(e) $\neg(p \wedge q)$ is _____

Definition 1.18. *The* **exclusive or** *(or* **XOR***) of p and q, denoted by $\boldsymbol{p \oplus q}$, is the proposition "***$\boldsymbol{p}$* **is true or** *$\boldsymbol{q}$* **is true, but not both***". The exclusive or of* ***p*** *and* ***q*** *is true when exactly one of* ***p*** *or* ***q*** *is true. Put another way, the exclusive or of* ***p*** *and* ***q*** *is true iff* ***p*** *and* ***q*** *have different truth values.*

Example 1.19. Let p be the proposition "$x > 10$" and q be the proposition "$x < 20$." Then $p \oplus q$ is the proposition "$x > 10$ or $x < 20$, but not both."

Note: *Notice that $\vee$ is an* **inclusive or***, meaning that it is true if both are true, whereas $\oplus$ is an* **exclusive or***, meaning it is false if both are true. The difference between $\vee$ and $\oplus$ is complicated by the fact that in English, the word "or" to can mean either of these depending on context. For instance, if your mother tells you "you can have cake or ice cream" she is likely using the exclusive or, whereas a prerequisite of "Math 110 or demonstrated competency with algebra" clearly has the inclusive or in mind.*

★**Exercise 1.20.** For each of the following, is the *or* inclusive or exclusive? Answer **OR** or **XOR** for each.

(a) _____ The special includes your choice of a salad or fries.

(b) _____ The list is empty or the first element is zero.

(c) _____ The first list is empty or the second list is empty.

(d) _____ You need to take probability or statistics before taking this class.

(e) _____ You can get credit for either Math 111 or Math 222.

★**Exercise 1.21.** Let p be "list 1 is empty" and q be "list 2 is empty." Explain the difference in meaning between $p \vee q$ and $p \oplus q$.

Answer _____

_____

_____

Note: *The* **Question** *examples are similar to the* **Evaluate** *ones except that they ask a specific question. Write down your answer in the space provided and then compare your answer with the one in the solutions.*

★**Question 1.22.** Let p be the proposition "$x < 5$" and q be the proposition "$x > 15$."

(a) Do the statements $p \vee q$ and $p \oplus q$ mean the same thing? Explain.

Answer _____

_____

(b) Practically speaking, are $p \vee q$ and $p \oplus q$ the same? Explain.

Answer _____

_____

XOR is not used as often as AND and OR in logical expressions in programs. Some languages have an XOR operator and some do not. The issue gets blurry because some languages, like Java, have an explicit Boolean type, while others, like C and C++, do not. All of these languages have a *bitwise XOR* operator, but this is not the same thing as a *logical XOR* operator. We will return to this topic later. In the next section we will see how to implement $\oplus$ using $\vee$, $\wedge$, and $\neg$.

Definition 1.23. *The* **conditional statement** *(or* **implies** *or* **implication***) involving p and q, denoted by $\boldsymbol{p \to q}$, is the proposition "***if $\boldsymbol{p}$, then $\boldsymbol{q}$***". It is false when $\boldsymbol{p}$ is true and $\boldsymbol{q}$ is false, and true otherwise. In the statement $\boldsymbol{p \to q}$, we call $\boldsymbol{p}$ the* **premise** *(or* **hypothesis** *or* **antecedent***) and $\boldsymbol{q}$ the* **conclusion** *(or* **consequence***).*

Example 1.24. Let p be "you earn at least 94%," and q be "you will receive an A." Then $p \to q$ is the proposition "If you earn at least 94%, then you will receive an A."

It is important to realize that $p \to q$ and $q \to p$ are not always equivalent.

Example 1.25. Let p be "you earn at least 94%," and q be "you will receive an A." Then $p \to q$ is the proposition "If you earn at least 94%, then you will receive an A," and $q \to p$ is the proposition "If you receive an A, then you earned at least 94%." Although they may sound equivalent, they are not. Consider the possibility that it is true that receiving at least 93% results in an A. Then $p \to q$ is true, but $q \to p$ is false.

★**Question 1.26.** Assume that the proposition "If you earn at least 94% in this class, then you will receive an A" is true.

(a) What grade will you get if you earn 94%? Explain.

Answer _____

_____

(b) If you receive an A, did you earn at least 94%? Explain.

Answer _____

_____

(c) If you don't earn 94%, does that mean you didn't get an A? Explain.

Answer _____

_____

Example 1.27. Translating between an English sentence and a mathematical expression can sometimes be tricky with conditional statements. Again, let p be "you earn at least 94%," and q be "you will receive an A." Then the sentence "You will receive an A whenever you earn at least 94%" is $p \to q$, and not $q \to p$ since it is expressing the same idea as the sentence "If you

earn at least 94%, you will receive an A."

Note: *The* **conditional** *statement is by far the one that is the most difficult to get a handle on for at least two reasons. First, the conditional statement $p \to q$ is not saying anything about p or q by themselves. It is only saying that if p is true, then q has to also be true. It doesn't say anything about the case that p is not true. This brings us to the second reason. Should $F \to T$ be true or false? Although it seems counterintuitive to some, it should be true. Again, $p \to q$ is telling us about the value of q when p is true (i.e., if p is true, the q* must be *true). What does it tell us if p is false? Nothing. As strange as it might seem, when p is false, the whole statement is true regardless of the truth value of q.*

If you are still confused, you can simply fall back on the formal definition: **$p \to q$ is false when p is true and q is false, and is true otherwise.** *In other words, if interpreting $p \to q$ as the English sentence "p implies q" is more harmful than helpful in understanding the concept, don't worry about why it doesn't make sense and just remember the definition.*[a]

[a] In mathematics, terms are usually chosen so they make sense immediately. Sometimes this is not possible (if the concept is very complicated or it doesn't relate to anything familiar). Sometimes a term is poorly defined but the definition sticks because of prior use. Sometimes it makes sense to some people and not to others, probably based on a person's background. I think this last possibility may be the reason in this case.

We will learn more about the conditional statements and statements related to it in the chapter on proofs where it is particularly relevant.

Definition 1.28. *The* **biconditional statement** *involving p and q, denoted by $\boldsymbol{p \leftrightarrow q}$, is the proposition "**$\boldsymbol{p}$ if and only if $\boldsymbol{q}$**" (or abbreviated as "**$\boldsymbol{p}$ iff $\boldsymbol{q}$**"). It is true when $\boldsymbol{p}$ and $\boldsymbol{q}$ have the same truth value, and false otherwise.*

Example 1.29. Let p be "you earn at least 94%," and q be "you receive an A." Then $p \leftrightarrow q$ is the proposition "You earn at least 94% if and only if you receive an A."

★**Question 1.30.** Assume that the proposition "You will receive an A if and only if you earn at least 94%" is true.

(a) What grade will you get if you earn 94%?

Answer _____

(b) If you receive an A, did you earn at least 94%?

Answer _____

(c) If you don't earn at least 94%, does that mean you didn't get an A?

Answer _____

Now let's bring all of these operations together with a few more examples.

Example 1.31. Let a be the proposition "I will eat my socks," b be "It is snowing," and c be "I will go jogging." Here are some compound propositions involving a, b, and c, written using these variables and operators and in English.

With Variables/Operators	In English
$(b \vee \neg b) \rightarrow c$	Whether or not it is snowing, I will go jogging.
$b \rightarrow \neg c$	If it is snowing, I will not go jogging.
$b \rightarrow (a \wedge \neg c)$	If it is snowing, I will eat my socks, but I will not go jogging.
$a \leftrightarrow c$	When I eat my socks I go jogging, and when I go jogging I eat my socks. *or* I eat my socks if and only if I go jogging.

★**Fill in the details 1.32.** Let p be the proposition "*Iron Man* is on TV," q be "I will watch *Iron Man*," and r be "I own *Iron Man* on DVD." Fill in the missing information in the following table.

With Variables/Operators	In English
$p \rightarrow q$	
	If I don't own *Iron Man* on DVD and it is on TV, I will watch it.
$p \wedge r \wedge \neg q$	
	I will watch *Iron Man* every time it is on TV, and that is the only time I watch it.
	I will watch *Iron Man* if I own the DVD.

1.1.3 Truth Tables

Sometimes we will find it useful to think of compound propositions in terms of *truth tables*.

Definition 1.33. *A* **truth table** *is a table that shows the truth value of a compound proposition for all possible combinations of truth assignments to the variables in the proposition. If there are n variables, the truth table will have 2^n rows.*

The truth table for $\neg$ is given in Table 1.1 and the truth tables for all of the other operators we just defined are given in Table 1.2. In the latter table, the first two columns are the possible values of the two variables, and the last 5 columns are the values for each of the two-variable compound propositions we just defined for the given inputs.

p	$\neg p$
T	F
F	T

Table 1.1: Truth table for $\neg$

p	q	$(p \wedge q)$	$(p \vee q)$	$p \oplus q$	$(p \to q)$	$(p \leftrightarrow q)$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Table 1.2: Truth tables for the two-variable operators

Example 1.34. Construct the truth table of the proposition $a \vee (\neg b \wedge c)$.

Solution: Since there are three variables, the truth table will have $2^3 = 8$ rows. Here is the truth table, with several helpful intermediate columns.

a	b	c	$\neg b$	$\neg b \wedge c$	$a \vee (\neg b \wedge c)$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	F	T
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	F	T	F	F

Note: *Notice that there are several columns in the truth table besides the columns for the variables and the column for the proposition we are interested in. These are "helper" or "intermediate" columns (those are not official definitions). Their purpose is simply to help us compute the final column more easily and without (hopefully) making any mistakes.*

★**Exercise 1.35.** Construct the truth table for $(p \to q) \wedge q$.

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

Note: *As long as all possible values of the variables are included, the order of the rows of a truth table does not matter. However, by convention one of two orderings is usually used. Since there is an interesting connection to the binary representation of numbers, let's take a closer look at this connection in the next example.*

Example 1.36 (Ordering the rows of a Truth Table)**.** Notice that the values of the variables can be used to construct an index for each row. We can do this by thinking of each T as a 1 and each F as a 0, and treating the columns as a binary number. The rows will then be listed

either in order or (more commonly) in reverse order. For instance, if there are three variables, we can think of it as shown in the following table.

a	b	c				index
T	T	T	1	1	1	7
T	T	F	1	1	0	6
T	F	T	1	0	1	5
T	F	F	1	0	0	4
F	T	T	0	1	1	3
F	T	F	0	1	0	2
F	F	T	0	0	1	1
F	F	F	0	0	0	0

This is the ordering you should follow so that you can easily check your answers with those in the solutions. It also makes grading your homework easier.

There is also a way of thinking about this recursively. Given an ordering for a table with n variables, we can compute an ordering for a table with $n+1$ variables as follows. Make two copies of the columns corresponding to the n variables, appending a T to the beginning of the first copy, and an F to the beginning of the second copy.

★**Exercise 1.37.** Construct the truth table of the proposition $(a \vee \neg b) \wedge c$. You're on your own this time to supply all of the details.

1.1.4 Precedence Rules

Consider the compound proposition $a \vee \neg b \wedge c$. Should this be interpreted as $a \vee (\neg b \wedge c)$, $(a \vee \neg b) \wedge c$, or even possibly $a \vee \neg(b \wedge c)$? Does it even matter? You already know that $3 + (4 * 5) \neq (3 + 4) * 5$, so it should not surprise you that where you put the parentheses in logical expressions matters, too. In fact, Example 1.34 gives the truth table for one of these and you just computed the truth table for another one in Exercise 1.37. If you compare them, you will see that they are not the same. The third interpretation is also different from both of these.

To correctly interpret compound propositions, the operators have an *order of precedence*. The order is $\neg$, $\wedge$, $\oplus$, $\vee$, $\rightarrow$, and $\leftrightarrow$. Also, $\neg$ has right-to-left associativity, all other operators listed have left-to-right associativity. Based on these rules, the correct way to interpret $a \vee \neg b \wedge c$ is $a \vee ((\neg b) \wedge c)$.

It is important to know the precedence rules for the logical operators (or at least be able to look it up) so you can properly interpret complex logical expressions. However, I generally prefer to always use enough parentheses to make it immediately clear, especially when I am writing code. It isn't difficult to remember that $\neg$ is first (that is, it always applies to what is immediately after it) so sometimes I don't use parentheses for it.

Example 1.38. According to the precedence rules, $\neg a \rightarrow a \vee b$ should be interpreted as $(\neg a) \rightarrow (a \vee b)$.

Example 1.39. According to the precedence rules, $a \wedge \neg b \rightarrow c$ should be interpreted as $(a \wedge (\neg b)) \rightarrow c$.

★**Exercise 1.40.** According to the precedence rules, how should $a \wedge b \vee c$ be interpreted?

Answer _____

★**Question 1.41.** Are $(a \wedge b) \vee c$ and $a \wedge (b \vee c)$ equivalent? Prove your answer.

Answer _____

_____

Note: *The next example is an* **Evaluate** *exercise. These exercises give a problem and then provide one or more solutions to the problem based on previous student solutions. Your job is to evaluate each solution by finding any mistakes. Mistakes include not only incorrect algebra and logic, but also unclear presentation, skipped steps, incorrect assumptions, over-simplification, etc. When you come across these examples you should write down every error you can find. Once you are pretty sure you know all of the problems (if there are any), compare your evaluation to the one given in the solutions. Note that sometimes the given solutions are correct!*

★**Evaluate 1.42.** According to the associativity rules, how should $a \rightarrow b \rightarrow c$ be interpreted?

Solution: It should be interpreted as $(a \rightarrow b) \rightarrow c$. However, $a \rightarrow (b \rightarrow c)$ is equivalent, so it really doesn't matter.

Evaluation _____

_____

1.2 Propositional Equivalence

We have already informally discussed two propositions being *equivalent*. In this section, we will formally develop the notion of what it means for two propositions to be *equivalent* (or, more formally, *logically equivalent*). We will also provide you with a list of the most important logical equivalences, along with some examples of some that aren't necessarily as important, but make interesting examples. But first, we need some new terminology.

Definition 1.43. *A proposition that is always true is called a* **tautology**. *One that is always false is a* **contradiction**. *Finally, one that is neither of these is called a* **contingency**.

Example 1.44. Assume that x is a real number.

(a) The proposition "$x < 0$" is a contingency since its truth depends on the value of x.

(b) The proposition "$x^2 < 0$" is a contradiction since it is false no matter what x is.

(c) The proposition "$x^2 \geq 0$" is a tautology since it is true no matter what x is.

★**Fill in the details 1.45.** State whether each of the following propositions is a tautology, contradiction, or contingency. Give a brief justification.

(a) $p \vee \neg p$ is a _____ since either p or $\neg p$ has to be true.

(b) $p \wedge \neg p$ is a _____ since _____.

(c) $p \vee q$ is a _____ since _____.

We will cover proofs more formally later, but for now we will informally introduce two proof techniques involving propositional logic. To prove something is a tautology, one must prove that it is always true. One way to do this is to show that the proposition is true for every row of the truth table. Another way is to argue (without using a truth table) that the proposition is always true, often using a *proof by cases*. This is exactly what it sounds like: consider every possibility, and show that in all cases we get true.

Example 1.46. Prove that $p \vee \neg p$ is a tautology.
Here are several proofs.

Proof 1: Since every row in the following truth table for $p \vee \neg p$ is T, it is a tautology.

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Proof 2: By definition of disjunction, if p is true, then $p \vee \neg p$ is true. On the other hand,

if p is false, $\neg p$ is true. In this case, $p \vee \neg p$ is still true, again by definition of disjunction. Since $p \vee \neg p$ is true regardless of the value of p, it is a tautology.

★**Evaluate 1.47.** Prove that $[p \wedge (p \to q)] \to q$ is a tautology.

Proof 1:

P	Q	$P \to Q$	$P \wedge (P \to Q)$	$P \wedge (P \to Q) \to Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Evaluation _____

_____

Proof 2: One way to show that $P \wedge (P \to Q) \to Q$ is indeed a tautology is by filling out a truth table, as follows:

P	Q	$P \to Q$	$P \wedge (P \to Q)$	$P \wedge (P \to Q) \to Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Since they all return true for $P \wedge (P \to Q) \to Q$, this proves that it is a tautology.

Evaluation _____

_____

_____

Proof 3: One way to prove that this is a tautology is to make a couple of assumptions. First, since we know that for any statement $x \to y$ where y is true, then x can be either true or false. So let us assume that Q is false for this case. From the left side of the statement, if P is true, we would have true and (true implies false), which is false, thus we would have false implies false, which is true, and if P is false, then we would have false and (false implies true), which comes out false. So in both cases where Q is false, the statement equals out to false implies false, which is true, thus all four cases are true, thereby proving that $P \wedge (P \to Q) \to Q$ is a tautology.

Evaluation _____

Proof 4: Since an implication can only be false when the premise is true and the conclusion is false, we only need to prove that this can't happen. So let's assume that $p \wedge (p \to q)$ is true but that q is false. Since $p \wedge (p \to q)$ is true, p is true and $p \to q$ is true (by definition of conjunction). But if p is true and q is false, $p \to q$ is false. This is a contradiction, so it must be the case that our assumption that $p \wedge (p \to q)$ is true but that q is false is incorrect. Since that was the only possible way for $p \wedge (p \to q) \to q$ to be false, it cannot be false. Therefore it is a tautology.

Evaluation

Proof 5: Because 'merica.

Evaluation

Now we are ready to move on to the main topic of this section.

Definition 1.48. *Let p and q be propositions. Then p and q are said to be* **logically equivalent** *if $p \leftrightarrow q$ is a tautology. An alternative (but equivalent) definition is that p and q are equivalent if they have the same truth table. That is, if they have the same truth value for all assignments of truth values to the variables.*

When p and q are equivalent, we write $\boldsymbol{p = q}$. An alternative notation is $\boldsymbol{p \equiv q}$.

Note: *$p = q$ is* **not** *a compound proposition. Rather it is a statement about the relationship between two propositions.*

There are many *logical equivalences* (or *identities/rules/laws*) that come in handy when working with compound propositions. Many of them (e.g. commutative, associative, distributive) will resemble the arithmetic laws you learned in grade school. Others are very different. The most common ones are given in Table 1.3.

We will provide proofs of some of these so you can get the hang of how to prove propositions are equivalent. One method is to demonstrate that the propositions have the same truth tables. That is, they have the same value on every row of the truth table. But just drawing a truth table isn't enough. A statement like "since p and q have the same truth table, $p = q$" is necessary to make a connection between the truth table and the equivalence of the propositions. Let's see a few examples.

Name	*Equivalence*
commutativity	$p \vee q = q \vee p$ $p \wedge q = q \wedge p$
associativity	$p \vee (q \vee r) = (p \vee q) \vee r$ $p \wedge (q \wedge r) = (p \wedge q) \wedge r$
distributive	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
identity	$p \vee F = p$ $p \wedge T = p$
negation	$p \vee \neg p = T$ $p \wedge \neg p = F$
domination	$p \vee T = T$ $p \wedge F = F$
idempotent	$p \vee p = p$ $p \wedge p = p$
double negation	$\neg(\neg p) = p$
DeMorgan's	$\neg(p \vee q) = \neg p \wedge \neg q$ $\neg(p \wedge q) = \neg p \vee \neg q$
absorption	$p \vee (p \wedge q) = p$ $p \wedge (p \vee q) = p$

Table 1.3: Common Logical Equivalences

Example 1.49. Prove the double negation law: $\neg(\neg p) = p$.

Proof: The following is the truth table for p and $\neg(\neg p)$.

p	$\neg p$	$\neg(\neg p)$
T	F	T
F	T	F

Since the entries for both p and $\neg(\neg p)$ are the same for every row, $\neg(\neg p) = p$. □

The two versions of De Morgan's Law are among the most important propositional equivalences. It is easy to make a mistake when trying to simplify expressions conditional statements, and a solid understanding of De Morgan's Laws goes a long way. Let's take a look at them.

Example 1.50. Prove the first version of DeMorgan's Law: $\neg(p \vee q) = \neg p \wedge \neg q$

Proof: We can prove this by showing that both expression have the same truth table. Below is the truth table for $\neg(p \vee q)$ and $\neg p \wedge \neg q$ (the gray columns).

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Since they are the same for every row of the table, $\neg(p \vee q) = \neg p \wedge \neg q$. □

★**Exercise 1.51.** Prove the second version of De Morgan's Law: $\neg(p \wedge q) = \neg p \vee \neg q$.

Proof _____

_____

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T					
T	F					
F	T					
F	F					

Truth tables aren't the only way to prove that two propositions are equivalent. You can also use other equivalences. Let's see an example.

Example 1.52. Prove the idempotent law $p \vee p = p$ by using the other equivalences.

Proof: It is easier to prove backwards ($p = p \vee p$). We have

$$\begin{aligned} p &= p \vee F && \text{(by identity)} \\ &= p \vee (p \wedge \neg p) && \text{(by negation)} \\ &= (p \vee p) \wedge (p \vee \neg p) && \text{(by distribution)} \\ &= (p \vee p) \wedge T && \text{(by negation)} \\ &= p \vee p && \text{(by identity)} \end{aligned}$$

Thus, $p \vee p = p$. □

★**Fill in the details 1.53.** Prove the idempotent law $p \wedge p = p$ by using the other equivalences.

Proof: Notice that

$$\begin{aligned} p &= \_\_\_\_\_ && \text{(by identity)} \\ &= \_\_\_\_\_ && \text{(by negation)} \\ &= \_\_\_\_\_ && \text{(by distributive)} \\ &= \_\_\_\_\_ && \text{(by negation)} \\ &= p \wedge p && \text{(by \_\_\_\_\_)} \end{aligned}$$

Thus, _____. □

Although it is helpful to specifically state which rules are being used at every step, it isn't always required.

Example 1.54. Prove that $(p \wedge q) \vee (p \wedge \neg q) = p$.

Proof: It is not too difficult to see that

$$(p \wedge q) \vee (p \wedge \neg q) = p \wedge (q \vee \neg q) = p \wedge T = p.$$

□

★**Exercise 1.55.** Use the other equivalences (not a truth table) to prove the Absorption laws.

(a) Prove that $p \vee (p \wedge q) = p$.
Proof:

(b) Prove that $p \wedge (p \vee q) = p$.
Proof:

One use of propositional equivalences is to simplify logical expressions.

Example 1.56. Simplify $\neg(p \vee \neg q)$.

Solution: Using DeMorgan's Law and double negation, we can see that

$$\neg(p \vee \neg q) = \neg p \wedge \neg(\neg q) = \neg p \wedge q.$$

Table 1.4 contains some important identities involving $\rightarrow$, $\leftrightarrow$, and $\oplus$. Since these operators are not always present in a programming language, identities that express them in terms of $\vee$, $\wedge$, and $\neg$ are particularly important.

$p \oplus q = (p \vee q) \wedge \neg(p \wedge q)$	$p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p)$
$p \oplus q = (p \wedge \neg q) \vee (\neg p \wedge q)$	$p \leftrightarrow q = \neg p \leftrightarrow \neg q$
$\neg(p \oplus q) = p \leftrightarrow q$	$p \leftrightarrow q = (p \wedge q) \vee (\neg p \wedge \neg q)$
$p \rightarrow q = \neg q \rightarrow \neg p$	$\neg(p \leftrightarrow q) = p \leftrightarrow \neg q$
$p \rightarrow q = \neg p \vee q$	$\neg(p \leftrightarrow q) = p \oplus q$

Table 1.4: Logical equivalences involving $\rightarrow$, $\leftrightarrow$, and $\oplus$

★**Exercise 1.57.** Let p be "$x > 0$", q be "$y > 0$," and r be "Exactly one of x or y is greater than 0."

(a) Express r in terms of p and q using $\oplus$ (and possibly $\neg$).

Answer _____

(b) Express r in terms of p and q *without using* $\oplus$.

Answer _____

Here is the proof of one of the identities from Table 1.4.

Example 1.58. Prove that $p \oplus q = (p \wedge \neg q) \vee (\neg p \wedge q)$.

Solution: It is straightforward to see that $(p \wedge \neg q) \vee (\neg p \wedge q)$ is true if p is true and q is false, or if p is false and q is true, and false otherwise. Put another way, it is true iff p and q have different truth values. But this is the definition of $p \oplus q$. Thus, $p \oplus q = (p \wedge \neg q) \vee (\neg p \wedge q)$.

The previous example demonstrates an important general principle. When proving identities (or equations of any sort), sometimes it works best to start from the right hand side. More generally, it is often best to start from the more complicated expression. Try to keep this in mind in the future.

★**Evaluate 1.59.** Show that $p \leftrightarrow q$ and $(p \wedge q) \vee (\neg p \wedge \neg q)$ are logically equivalent.

Proof 1: p ↔ q is true when p and q are both true, and so is (p ∧ q) ∨ (¬p ∧ ¬q). Therefore they are logically equivalent.

Evaluation _____

Proof 2: They are both true when p and q are both true or both false. Therefore they are logically equivalent.

Evaluation _____

Proof 3: Each of these is true precisely when p and q are both true.

Evaluation _____

Proof 4: Each of these is true when p and q have the same truth value and false otherwise, so they are equivalent.

Evaluation _____

In the previous example, you should have noticed that just a subtle change in wording can be the difference between a correct or incorrect proof. When writing proofs, remember to be very precise in how you word things. You may know what you mean when you wrote something, but a reader can only see what you actually wrote.

1.3 Predicates and Quantifiers

Definition 1.60. *A* **predicate** *or* **propositional function** *is a statement containing one or more variables, whose truth or falsity depends on the value(s) assigned to the variable(s).*

We have already seen predicates in previous examples. Let's revisit one.

Example 1.61. In a previous example we saw that "$x < 0$" was a contingency, "$x^2 < 0$" was a contradiction, and "$x^2 \geq 0$" was a tautology. Each of these is actually a predicate since until we assign a value to x, they are not propositions.

Sometimes it is useful to write *propositional functions* using functional notation.

Example 1.62. Let $P(x)$ be "$x < 0$". Notice that until we assign some value to x, $P(x)$ is neither true nor false.

$P(3)$ is the proposition "$3 < 0$," which is false.

If we let $Q(x)$ be "$x^2 \geq 0$," then $Q(3)$ is "$3^2 \geq 0$," which is true.

Notice that both $P(x)$ and "$x < 0$" are propositional functions. In other words, we don't have to use functional notation to represent a propositional function. Any statement that has a variable in it is a propositional function, whether we label it or not.

★**Exercise 1.63.** Which of the following are propositional functions?

(a) ___ $x^2 + 2x + 1 = 0$

(b) ___ $3^2 + 2 \cdot 3 + 1 = 0$

(c) ___ John Cusack was in movie M.

(d) ___ x is an even integer if and only if $x = 2k$ for some integer k.

Definition 1.64. *The symbol* $\forall$ *is the* **universal quantifier***, and it is read as "for all", "for each", "for every", etc. For instance,* $\forall x$ *means "for all* x*". When it precedes a statement, it means that the statement is true* for all values of x.

As the name suggests, the "all" refers to everything in the **universe of discourse** *(or* **domain of discourse***, or simply* **domain***), which is simply the set of objects to which the current discussion relates.*

Hopefully you recall that $\mathbb{N}$ is the set of natural numbers (i.e. $\{0, 1, 2, \ldots\}$), $\mathbb{Z}$ is the set of integers, and $\mathbb{Z}^+$ is the set of positive integers (i.e. $\{1, 2, 3, \ldots\}$). We will use these in some of the following examples.

Example 1.65. Let $P(x)$="$x < 0$". Then $P(x)$ is a propositional function, and $\forall x P(x)$ means "all values of x are negative." If the domain is $\mathbb{Z}$, $\forall x P(x)$ is false. However, if the domain is negative integers, $\forall x P(x)$ is true.

Example 1.66. Express each of the following English sentences using the universal quantifier. Don't worry about whether or not the statements are true. Assume the domain is real numbers.

(a) The square of every number is non-negative.

(b) All numbers are positive.

Solution: (a) $\forall x(x^2 \geq 0)$ (b) $\forall x(x > 0)$

★**Exercise 1.67.** Express each of the following using the universal quantifier. Assume the domain is $\mathbb{Z}$.

(a) Two times any number is less than three times that number.

Answer _____

(b) $n!$ is always less than n^n.

Answer _____

Example 1.68. The expression $\forall x(x^2 \geq 0)$ means "for all values of x, x^2 is non-negative". But what constitutes *all* values? In other words, what is the domain? In this case the most logical possibilities are the integers or real numbers since it seems to be stating something about numbers (rather than people, for example). In most situations the context should make it clear what the domain is.

Example 1.69. The expression $\forall x \geq 0, x^3 \geq 0$ means "for all positive values of x, $x^3 \geq 0$." There are several other ways of expressing this idea, but this one is probably the most convenient. One alternative would be to restrict the domain to positive numbers and write it as $\forall x(x^3 \geq 0)$. But sometimes you don't want to or can't restrict the domain.

Another way to express it is $\forall x(x \geq 0 \rightarrow x^3 \geq 0)$.

★**Exercise 1.70.** Use the universal quantifier to express the fact that the square of any integer is not zero as long as the integer is not zero.

Answer _____

Definition 1.71. *The symbol* $\exists$ *is the* **existential quantifier**, *and it is read as "there exists", "there is", "for some", etc. For instance,* $\exists x$ *means "For some* x*". When it precedes a statement, it means that the statement is true for* at least one value of x *in the universe.*

Example 1.72. Prove that $\exists x(\sqrt{x} = 2)$ is true when the domain is the integers.

Proof. Notice that when $x = 4$, $\sqrt{x} = \sqrt{4} = 2$, proving the statement. □

★**Exercise 1.73.** Express the sentence "Some integers are positive" using quantifiers. You may assume the domain of the variable(s) is $\mathbb{Z}$.

Answer _____

Sometimes you will see *nested quantifiers*. Let's see a few examples.

Example 1.74. Use quantifiers to express the sentence "all positive numbers have a square root," where the domain is real numbers.

Solution: We can express this as $\forall(x > 0)\exists y(\sqrt{x} = y)$.

★**Evaluate 1.75.** Express the sentence "Some integers are even" using quantifiers. You may assume the domain of the variable(s) is the integers.

Solution 1: $\exists x$(x is even).

Evaluation _____

_____

Solution 2: $\exists x(x/2 \in \mathbb{Z})$.

Evaluation _____

_____

Solution 3: $\exists x \exists y(x = 2y)$.

Evaluation _____

_____

Example 1.76. Translate $\forall\forall\exists\exists$ into English.

Solution: It means "*for every upside-down A there exists a backwards E*." This is a geeky math joke that might make sense if you paid attention in calculus (assuming you ever took calculus, of course).

★**Exercise 1.77.** Express the following statement using quantifiers: "Every integer can be expressed as the sum of two squares." Assume the domain for all three variables (did you catch the hint?) is $\mathbb{Z}$.

Answer _____

★**Exercise 1.78.** Find a predicate $P(x, y)$ such that $\forall x \exists y P(x, y)$ and $\exists y \forall x P(x, y)$ have different true values. Justify your answer. (Hint: Think simple. Will something like "$x = y$" or "$x < y$" work if you choose the appropriate domain?)
Answer:

Example 1.79. Let $P(x)$="$x < 0$". Then $\neg \forall x P(x)$ means "it is not the case that all values of x are negative." Put more simply, it means "some value of x is not negative", which we can write as $\exists x \neg P(x)$.

What we saw in the last example actually holds for any propositional function.

Theorem 1.80 (DeMorgan's Laws for quantifiers)**.** *If $P(x)$ is a propositional function, then*

$$\neg \forall x P(x) = \exists x \neg P(x), \text{ and}$$

$$\neg \exists x P(x) = \forall x \neg P(x).$$

Proof: *We will prove the first statement. The proof of the second is very similar. Notice that $\neg \forall x P(x)$ is true if and only if $\forall x P(x)$ is false. $\forall x P(x)$ is false if and only if there is at least one x for which $P(x)$ is false. This is true if and only if $\neg P(x)$ is true for some x. But this is exactly the same thing as $\exists x \neg P(x)$, proving the result.* □

Example 1.81. Negate the following expression, but simplify it so it does not contain the $\neg$ symbol.

$$\forall n \exists m (2m = n)$$

Solution:

$$\begin{aligned} \neg\forall n \exists m (2m = n) &= \exists n \neg \exists m (2m = n) \\ &= \exists n \forall m \neg (2m = n) \\ &= \exists n \forall m (2m \neq n) \end{aligned}$$

★**Exercise 1.82.** Answer the following questions about the expression from Example 1.81, assuming the domain is $\mathbb{Z}$.

(a) Write the expression in English. You can start with a direct translation, but then smooth it out as much as possible.

Answer _____

_____

(b) Write the negation of the expression in English. State it as simply as possible.

Answer _____

_____

(c) What is the truth value of the expression? Prove it.

Answer _____

_____

1.4 Normal Forms

Earlier we saw identities that express logical operators in terms of $\vee$, $\wedge$, and $\neg$. It turns out that even if there isn't an identity that does it, there is a straightforward technique to convert any logical expression into one only using $\vee$, $\wedge$, and $\neg$. That is the topic of this section.

Specifically, we will introduce two standard forms that every boolean expression can be written in: *disjunctive normal form* and *conjunctive normal form*. These form have connections to important areas of computer science including circuit design and minimization, artificial intelligence algorithms, automated theorem proving, and the study of algorithm complexity. We begin with a few necessary definitions.

Definition 1.83. *A* **literal** *is a boolean variable or its negation.*

Example 1.84. Let p, q, and r be boolean variables. Then p, $\neg p$, q, $\neg q$, r, and $\neg r$ are all literals.

On the other hand, $p \wedge q$, $\neg p \rightarrow q$, and $p \wedge q \wedge r$ are *not* literals because they include boolean operations of two or more variables. In other words, none of them are a variable or the negation of a variable.

★**Exercise 1.85.** Let p, q, and r be boolean variables. Which of the following are literals? $q \vee r$, $\neg p$, q, $p \wedge q \wedge r$, $\neg p \wedge q$, r.

Answer _____

_____

Definition 1.86. *A* **conjunctive clause** *is a conjunction (*AND*) of one or more literals.*

Example 1.87. Let p, q, and r be boolean variables. Then $p \wedge q \wedge r$, $\neg p \wedge r$, and $r \wedge \neg q \wedge p$ are all conjunctive clauses.

$\neg(p \wedge q)$ is not a conjunctive clause because it has a negation that is applied to the conjunction and not to just a variable. Other examples that are *not* conjunctive clauses are $p \vee r$, $p \vee q \wedge r$, $p \leftrightarrow r$, and $p \wedge q \wedge (r \oplus p)$.

Example 1.88. Literals are conjunctive clauses since they are a conjunction of a single variable. This might sound weird because if you only have a single variable, there is nothing to "conjoin" it to. But it is just like if someone asked to to add up all of the money in your pocket–if you only have a single dollar, you will say you have one dollar, having "added up" the dollar.

Therefore, p, $\neg p$, q, $\neg q$, r, and $\neg r$ are all conjunctive clauses.

★**Exercise 1.89.** Let p, q, and r be boolean variables. Which of the following are conjunctive clauses?
$q \vee r$, $\neg p$, q, $p \wedge q \wedge r$, $\neg p \to q$, $\neg p \wedge q$, r, $\neg r \wedge p \wedge q$, $q \vee \neg r$, $p \wedge \neg(r \wedge q)$

Answer _____

_____

Definition 1.90. *A logical expression is in* **disjunctive normal form** *(***DNF***) (or* **sum-of-products expansion***) if it is expressed as a disjunction (*OR*) of conjunctive clauses.*

Example 1.91. Let p, q, and r be boolean variables. Then the following are in disjunctive normal form:

- q (It is the disjunction of a single conjunctive clause that consists of just a literal.)
- $p \wedge \neg q$ (It is the disjunction of a single conjunctive clause.)
- $p \vee \neg q$ (It is the disjunction of two conjunctive clauses, each of which is just a literal.)
- $(p \wedge q \wedge r) \vee (\neg p \wedge r)$
- $p \vee (q \wedge \neg p) \vee (r \wedge \neg p)$
- $r \wedge \neg q \wedge p$

These are *not* in disjunctive normal form.

- $p \to q$
- $p \wedge (q \vee r)$
- $p \vee \neg(r \wedge q)$
- $p \vee (q \wedge \neg p) \wedge (r \vee \neg q)$
- $(p \leftrightarrow q) \vee (q \wedge \neg r) \vee \neg p$

★**Exercise 1.92.** Let p, q, and r be boolean variables. Which of the following are in disjunctive normal form?
$\neg p$, $q \vee r$, $\neg q \wedge r$, $p \wedge q \wedge r$, $(\neg p \to q) \vee (q \wedge r)$, $\neg(p \wedge \neg q)$, $\neg r \wedge p \wedge q$, $\neg(p \vee q)$, $p \wedge \neg(r \wedge q)$, $(p \wedge \neg r) \vee (r \wedge q) \vee (\neg q \wedge p)$, $(p \vee \neg r) \wedge (r \vee q) \wedge (\neg q \vee p)$, $(p \wedge \neg r) \vee (r \vee q) \vee (\neg q \wedge p)$, $(p \wedge \neg r) \vee (r \wedge q) \wedge (\neg q \wedge p)$, $(p \wedge \neg r) \vee (r \wedge q) \vee (\neg q \wedge p \wedge r)$

Answer _____

_____

Make sure you have a clear understanding of when an expression is and is not a literal, a conjunctive clause, or in disjunctive normal form.

Now you understand what disjunctive normal form is and can recognize when an expression is in this form. Next we describe how to convert any expression to an equivalent one that is in disjunctive normal form. The procedure involves constructing a truth table for the expression. The process is pretty straightforward once you get the hang of it, but it can be a little tricky at first so pay careful attention!

Procedure 1.93. *This will convert a boolean expression to disjunctive normal form.*

1. *Create a truth table for the expression.*
2. *Identify the rows having output T.*
3. *For each such row, create a conjunctive clause that includes all of the variables which are true on that row and the negation of all of the variables that are false.*
4. *Combine all of the conjunctive clauses by disjunctions.*

Example 1.94. Express $p \oplus q$ in disjunctive normal form.

Solution: The truth table for $p \oplus q$ is given to the right. The second and third rows of the table are true, so we use those to construct the disjunctive normal form.

The second row yields conjunctive clause $p \wedge \neg q$, and the third row yields conjunctive clause $\neg p \wedge q$. The disjunction of these is $(p \wedge \neg q) \vee (\neg p \wedge q)$.
Thus, $p \oplus q = (p \wedge \neg q) \vee (\neg p \wedge q)$.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

The previous example is essentially just another proof of the identity that was proven in Example 1.58.

★**Exercise 1.95.** Express $p \leftrightarrow q$ in disjunctive normal form.

p	q	$p \leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

Example 1.96. Express Z in disjunctive normal form.

p	q	r	Z
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

Solution: $Z = (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r)$.

The solution from the previous example can be simplified to $Z = (p \wedge q) \vee (\neg p \wedge \neg r)$. Although this can be done by applying the logical equivalences we learned about earlier, there are more sophisticated techniques that can be used to simplify expressions that are in disjunctive normal form. This is beyond our scope, but you may learn more about this if you take a computer organization class and discuss circuit minimization. The important point I want to make here is that computing the disjunctive normal form of an expression using the technique we describe will not always produce the most simple form of the expression. In fact, most of the time it won't be.

★**Exercise 1.97.** Express Y in disjunctive normal form.

p	q	r	Y
T	T	T	F
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	T
F	F	F	T

There is another important form that is very similar to disjunctive normal form.

Definition 1.98. *A* **disjunctive clause** *is a disjunction (*OR*) of one or more literals. A logical expression is in* **conjunctive normal form** *(***CNF***) (or* **product-of-sums expansion***) if it is expressed as a conjunction (*AND*) of disjunctive clauses.*

There are several methods for converting to conjunctive normal form. They generally involve using double negation, distributive, and De Morgan's laws either based on the truth table or based on the disjunctive normal form. However, we won't discuss these techniques here.

1.5 Reading Comprehension Questions

Note: *It is recommended that you attempt to complete* all *of the questions before checking your answers. As with the exercises throughout the book, it is also recommended that if you get one wrong, attempt to solve it again before reading the answer/solution in detail. You will learn a lot more that way!*

Also, the solutions given are often just one possible answer (especially when answers involve coming up with an example). If your answer is different, you should be able to determine whether or not your answer is also correct. If you are not sure, please ask!

From Section 1.1

★**Question 1.1.** What is a proposition?

★**Question 1.2.** What are the six logical operators that were introduced in this chapter? Draw a truth table for each.

★**Question 1.3.** Explain the difference between *(inclusive) or* and *exclusive or*.

★**Question 1.4.** When is $p \to q$ true?

★**Question 1.5.** Draw a truth table for $(p \wedge q) \vee \neg p$.

★**Question 1.6.** Draw a truth table for $(p \wedge q) \vee r$.

★**Question 1.7.** Can p and $\neg p$ both be true? Explain.

★**Question 1.8.** If $p \vee q$ is true and p is false, what can you say about q?

★**Question 1.9.** If $p \vee q$ is true and p is true, what can you say about q?

★**Question 1.10.** If $p \wedge q$ is true, what can you say about p and/or q?

★**Question 1.11.** If $p \leftrightarrow q$ is true and p is false, what can you say about q?

★**Question 1.12.** If $p \to q$ is true and p is true, what can you say about q?

★**Question 1.13.** If $p \to q$ is true and p is false, what can you say about q?

From Section 1.2

★**Question 1.14.** Can a proposition be a contingency and a tautology at the same time?

★**Question 1.15.** Is it possible for both a proposition and its negation to be true? Explain.

★**Question 1.16.** Prove the domination laws. That is, prove that

(a) $p \vee T = T$

(b) $p \wedge F = F$.

★**Question 1.17.** Explain why $\neg p \wedge \neg q$ and $\neg(p \wedge q)$ are not logically equivalent.

★**Question 1.18.** Why is "because that's not what DeMorgan's law says" or "because they look different" not sufficient to prove that $\neg p \wedge \neg q$ and $\neg(p \wedge q)$ are not logically equivalent.

★**Question 1.19.** What is an easy way to prove that two propositions are not logically equivalent?

From Section 1.3

★**Question 1.20.** What is a propositional function (or predicate)? Give an example.

★**Question 1.21.** Does $\neg\forall x P(x)$ mean $P(x)$ is never true? If so, convince me. If not, what does it mean?

★**Question 1.22.** Does $\neg\exists x P(x)$ mean $P(x)$ is never true? If so, convince me. If not, what does it mean?

★**Question 1.23.** Give two equivalent (but different) ways of expressing $\forall x \neg\exists y Q(x, y)$.

★**Question 1.24.** Give three equivalent (but different) ways of expressing $\neg\exists x(x < 0 \wedge x > 0)$.

★**Question 1.25.** Express the sentence "Everybody hurts sometimes" using predicates and quantifiers. To get you started, let $H(x, y) =$"x hurts at time y".

★**Question 1.26.** Express the sentence "Nothing ever changes, nothing ever stays the same" using predicates and quantifiers. Hint: You will need to define one or two predicates, depending on how you interpret the sentence and how clever you are.

★**Question 1.27.** Let $P(x, y) =$"$x \leq y$" and assume the universe of discourse is the set of integers.

(a) Rephrase $\forall x \exists y P(x, y)$ in English.

(b) Rephrase $\exists x \forall y P(x, y)$ in English.

(c) Do the statements in parts (a) and (b) seem to be saying the same thing? Explain.

(d) What is the truth value of $\forall x \exists y P(x, y)$?

(e) What is the truth value of $\exists x \forall y P(x, y)$?

(f) Hopefully you answered that one of the statements is true and the other is false (If not, go back to the previous two questions and try again!). Can you change the universe of discourse so that the two statements have the same truth values?

(g) If you said no to the previous question, go back and try harder before continuing. So, you can make them have the same truth value by changing the universe of discourse. Does that mean with this universe of discourse the statement are saying the same thing? (This is a subtle but important point, so if you are not totally confident in your answer, ask about this one!)

From Section 1.4

★**Question 1.28.** Let p, q and r be boolean variables. Which of the following are literals? $\neg p$, $\neg p \wedge r$, q, $\neg r$, $p \to r$, r.

★**Question 1.29.** Let p, q and r be Boolean variables. Which of the following are conjunctive clauses? $\neg p$, $p \wedge r$, $q \vee \neg r$, $\neg p \wedge r$, q, $\neg r$, $p \to r$, $\neg(p \wedge q)$.

★**Question 1.30.** Let p, q and r be Boolean variables. Which of the following are in disjunctive normal form? $\neg p$, $p \wedge r$, $q \vee \neg r$, $\neg p \wedge r$, $p \to r$, $\neg(p \wedge q)$, $(p \wedge q) \vee (q \wedge \neg r) \vee \neg p$, $(p \vee q) \wedge (q \vee \neg r) \wedge \neg p$, $(p \wedge r) \vee \neg(r \wedge \neg q) \vee (\neg p \wedge q)$, $(p \wedge \neg r \wedge q) \vee (\neg p \wedge r \wedge \neg q) \vee (p \wedge r \wedge q) \vee (\neg p \wedge \neg r \wedge \neg q)$.

1.6 Problems

Problem 1.1. Draw a truth table to represent the following.

(a) $\neg p \vee q$

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

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

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

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

(f) $(p \oplus q) \wedge (q \vee r)$

(g) $p \leftrightarrow (p \wedge q)$

Problem 1.2. Prove the distributive laws.

(a) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

(b) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

Problem 1.3. Prove the identity laws.

(a) $p \vee F = p$

(b) $p \wedge T = p$

Problem 1.4. Prove the negation laws.

(a) $p \vee \neg p = T$

(b) $p \wedge \neg p = F$

Problem 1.5. Prove that $p \oplus q = (p \vee q) \wedge \neg(p \wedge q)$.

Problem 1.6. Prove the following laws involving implications.

(a) $p \to q = \neg p \vee q$

(b) $p \to q = \neg q \to \neg p$

Problem 1.7. Prove the following laws involving biconditionals.

(a) $p \leftrightarrow q = (p \to q) \wedge (q \to p)$

(b) $p \leftrightarrow q = \neg p \leftrightarrow \neg q$

(c) $\neg(p \leftrightarrow q) = p \leftrightarrow \neg q$

Problem 1.8. Give 2 different proofs that $[(p \vee q) \wedge \neg p] \to q$ is a tautology.

Problem 1.9. Prove $\neg(p \leftrightarrow q) = p \oplus q$ without using truth tables.

Problem 1.10. Express $p \vee q \vee r$ using only $\wedge$ and $\neg$.

Problem 1.11. The *NAND* of p and q, denoted by $p|q$, is the proposition "not both p and q". The NAND of p and q is false when p and q are both true and true otherwise.

(a) Draw a truth table for $NAND$

(b) Express $p|q$ using $\vee$, $\wedge$, and/or $\neg$ (you may not need all of them).

(c) Express $p \wedge q$ using *only* $|$. (That means you cannot use $\neg$, $\vee$, $\wedge$, or any other boolean operator except for $|$. Thus, your answer should *only* involve p, q, $|$ and parentheses.) Your answer should be as simple as possible. Give a truth table that shows they are the same.

(d) Express $\neg p \vee q$ using only $|$. Your answer should be as simple as possible. Give a truth table that shows they are the same.

Problem 1.12. The *NOR* of p and q, denoted by $p \downarrow q$, is the proposition "neither p nor q". The NOR of p and q is true when p and q are both false and false otherwise.

(a) Draw a truth table for $\downarrow$

(b) Express $p \downarrow q$ using $\vee$, $\wedge$, and/or $\neg$ (you may not need all of them).

(c) Express $p \wedge q$ using *only* $\downarrow$. (That means you cannot use $\neg$, $\vee$, $\wedge$, or any other boolean operator except for $\downarrow$. Thus, your answer should *only* involve p, q, $\downarrow$ and parentheses.) Your answer should be as simple as possible. Give a truth table that shows they are the same.

(d) Express $\neg p \vee q$ using only $\downarrow$. Your answer should be as simple as possible. Give a truth table that shows they are the same.

Problem 1.13. A set of logical operators is *functionally complete* if any possible operator can be implemented using only operators from that set. It turns out that $\{\neg, \wedge\}$ is functionally complete. So is $\{\neg, \vee\}$. To show that a set if functionally complete, all one needs to do is show how to implement all of the operators from another functionally complete set. Given this,

(a) Show that $\{|\}$ is functionally complete. (Hint: Since $\{\neg, \wedge\}$ is functionally complete, one way is to show how to implement both $\wedge$ and $\neg$ using just $|$.)

(b) Show that $\{\downarrow\}$ is functionally complete.

Problem 1.14. Express the following phrase using quantifiers. "There is some constant c such that $f(x)$ is no greater than $c \cdot g(x)$ for all $x \geq x_0$ for some constant x_0." Your solution should contain no English words.

Problem 1.15. Write each of the following expressions so that negations are only applied to propositional functions (and not quantifiers or connectives).

(a) $\neg\forall x \exists y \neg P(x, y)$

(b) $\neg(\forall x \exists y P(x, y) \wedge \exists x \neg \forall y P(x, y))$

(c) $\neg\forall x(\exists y P(x, y) \vee \forall y Q(x, y))$

(d) $\neg\forall x \neg \exists y(\neg\forall z P(x, z) \rightarrow \exists z Q(x, y, z))$

(e) $\neg\exists x(\neg\forall y[\exists z(P(y, x, z) \wedge P(y, z, x) \wedge P(x, y, z))] \vee \exists z Q(x, z))$

Problem 1.16. Let $P(x, y)$="x likes y", where the universe of discourse for x and y is the set of all people. Translate each of the following into English, smoothing them out as much as possible. Then give the truth value of each.

(a) $\forall x \forall y P(x, y)$

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

(c) $\forall y \exists x P(x, y)$

(d) $\forall x P(x, Raymond)$

(e) $\neg \forall x \forall y P(x, y)$

(f) $\forall x \neg \forall y P(x, y)$

(g) $\forall x \neg \forall y \neg P(x, y)$

Problem 1.17. Let $P(x, y, z)$="$x^2 + y^2 = z^2$", where the universe of discourse for all variables is the set of integers. What are the truth values of each of the following?

(a) $\forall x \forall y \forall z P(x, y, z)$

(b) $\exists x \exists y \forall z P(x, y, z)$

(c) $\forall x \exists y \exists z P(x, y, z)$

(d) $\forall x \forall y \exists z P(x, y, z)$

(e) $\forall x \exists y \forall z P(x, y, z)$

(f) $\exists x \exists y \exists z P(x, y, z)$

(g) $\exists z P(2, 3, z)$

(h) $\exists x \exists y P(x, y, 5)$

(i) $\exists x \exists y P(x, y, 3)$

Problem 1.18. Write each of the following sentences using quantifiers and propositional functions. Define propositional functions as necessary (e.g. Let $D(x)$ be the proposition 'x plays disc golf.')

(a) All disc golfers play ultimate Frisbee.

(b) If all students in my class do their homework, then some of the students will pass.

(c) If none of the students in my class study, then all of the students in my class will fail.

(d) Not everybody knows how to throw a Frisbee 300 feet.

(e) Some people like ice cream, and some people like cake, but everybody needs to drink water.

(f) Everybody loves somebody.

(g) Everybody is loved by somebody.

(h) Not everybody is loved by everybody.

(i) Nobody is loved by everybody.

(j) You can't please all of the people all of the time, but you can please some of the people some of the time.

(k) If only somebody would give me some money, I would buy a new house.

(l) Nobody loves me, everybody hates me, I'm going to eat some worms.

(m) Every rose has its thorn, and every night has its dawn.

(n) No one ever is to blame.

Problem 1.19. Consider the following expression:

$$\forall \epsilon{>}0\, \exists \delta{>}0\, \forall x (0 < |x - c| < \delta \to |f(x) - L| < \epsilon).$$

(a) Express it in English. Be as concise as possible.

(b) (Difficult if you have not had calculus.) This is the definition of something. What is it?

Problem 1.20. Use Procedure 1.93 to find the disjunctive normal form for each of the expressions from Problem 1.1.

Chapter 2: Proof Methods

The ability to write proofs is important. Although you may not find yourself writing proofs on a regular basis in your future career, you will certainly need to make arguments based on evidence and logic. Proof writing is exactly that, although it is typically more formal, and the subjects of our proofs are generally mathematical. Nevertheless, what you learn here is definitely applicable way beyond writing mathematical proofs of simple mathematical results (which will be the focus of our proof writing).

In this chapter we will introduce you to the basics of mathematical proofs. Along the way we will review some mathematical concepts/definitions you have probably already seen, and introduce you to some new ones that we will find useful as we proceed. We will continue to write proofs and learn more advanced proof techniques as the book continues.

2.1 Direct Proofs

A *direct proof* is one that follows from the definitions. Facts previously learned help many a time when writing a direct proof. We will begin by seeing some direct proofs about something you should already be very familiar with: even and odd integers.

Definition 2.1. *Recall that:*

- *An* **even integer** *is one of the form* $2k$*, where* k *is an integer.*
- *An* **odd integer** *is one of the form* $2k+1$ *where* k *is an integer.*
- *Two integers have the same* **parity** *if they are both even or both odd.*

Example 2.2. Use the definition of even to prove that the sum of two even integers is even.

Proof: If x and y are even, then $x = 2a$ and $y = 2b$ for some integers a and b. Then $x + y = 2a + 2b = 2(a + b)$, which is even since $a + b$ is an integer. □

Example 2.3. Use the definitions of even and odd to prove that the sum of an even integer and an odd integer is odd.

Proof: Let a be an even integer and b be an odd integer. Then $a = 2f$ and $b = 2g + 1$ for some integers f and g. Then $a + b = 2f + (2g + 1) = 2(f + g) + 1$. Since $f + g$ is an integer, $a + b$ is an odd integer. □

★**Fill in the details 2.4.** Use the definitions of even and odd to prove that the sum of two odd integers is even.

Proof: If x and y are odd, then $x = 2c+1$ and $y =$ _____ for some integers

c and d. Then $x+y = 2c+1+2d+1 = 2(c+d+1)$. Now _____ is an integer,

so $2(c+d+1)$ is an _____ integer. □

Example 2.5. Use the definitions of even and odd to prove that the product of two odd integers is odd.

Proof: Let a and b be odd integers. Then $a = 2l+1$ and $b = 2m+1$ for some integers l and m. Then $a \cdot b = (2l+1)(2m+1) = 4ml+2l+2m+1 = 2(2ml+l+m)+1$ which is odd since $2ml+m+l$ is an integer. □

★**Fill in the details 2.6.** Use the definitions of even and odd to prove that the product of an even integer and an odd integer is even.

Proof: Let a be an even integer and b be an odd integer. Then $a =$ _____

and $b =$ _____ for _____. Given that, we can see that $a \cdot b =$

$(2n)(2o+1) =$ _____. Since _____ is an integer, $a \cdot b$

is _____. □

These examples may seem somewhat ridiculous since they are proving such obvious facts. However, keep in mind that our goal is to learn techniques for writing proofs. As we proceed the proofs will become more complicated, but we will continue to follow the same basic techniques we are using here. In other words, the fact that we are proving facts about even and odd integers is not at all important. What is important are the techniques we are learning in the process.

You may be asking yourself "why are we wasting our time proving such obvious results"? If so, ask yourself this: Would you rather be asked to prove more complicated things right away?

Think about how you learned to read and write. You started by reading books that only had a few simple words. As you progressed, the books and the words in them got longer. The vocabulary increased. You encountered increasingly complex sentence and paragraph structures. The same is true when you learned to write. You began by writing the letters of the alphabet. Then you learned to write words, followed by sentences, paragraphs, and eventually essays.

Learning to read and write proofs follows the same procedure. In order to know how to write correct proofs you first need to see some examples of them. But you need to go beyond just seeing them–you need to *understand* them. That is the goal of examples like the previous one. Your brain needs to be engaged with the material as you work through the book. You *must* work through all of the examples in order to get the most out of this book.

★**Exercise 2.7.** Use the definition of even to prove that the product of two even integers is even.
Proof:

★**Evaluate 2.8.** Evaluate the following proof that supposedly uses the definition of odd to prove that the product of two odd integers is odd.

> Proof: By definition of odd numbers, let a be an odd integer $2n+1$ let b be an odd integer $2q+1$. Then $(2n+1)(2q+1) = 4nq+2n+1 = 2(2nq+1)+1$. Since $2nq+1$ is an integer, $2(2nq+1)+1$ is an odd integer by definition of odd. □

Evaluation _____

Sometimes students get frustrated because they think that too many details are required in a proof. Why are mathematicians such sticklers on the details? The next example is the first of many that will try to demonstrate why the seemingly little details matter.

★**Question 2.9.** What is wrong with the following "proof" that the sum of an even and an odd number is even?

> Proof: Let $a=2n$ be an even integer and $b = 2m+1$ be an odd integer. Then $a + b = 2n + 2m + 1 = 2(n + m + 1/2)$. Since we wrote $a + b$ as a multiple of 2, it is even. Therefore the sum of an even and an odd number is even. □

Answer _____

We will find the following definitions useful throughout the book.

Definition 2.10. *Let b and a be integers with $a \neq 0$. We say that b is* **divisible by** *a if there exists an integer c such that $b = ac$. If b is divisible by a, we also say that b is a* **multiple** *of a, a is a* **factor** *or* **divisor** *of b, and that a* **divides** *b, written as $a|b$. If a does not divide b, we write $a \nmid b$.*

Example 2.11. Since $6 = 2 \cdot 3$, $2|6$, and $3|6$. But $4 \nmid 6$ since we cannot write $6 = 4 \cdot c$ for any integer c.

Example 2.12. Prove that the product of two even integers is divisible by 4.

Proof: Let $2h$ and $2k$ be even integers. Then $(2h)(2k) = 4(hk)$. Since hk is an integer, $4(hk)$ is divisible by 4. □

★**Fill in the details 2.13.** Prove that if x is an integer and 7 divides $3x + 2$, then 7 also divides $15x^2 - 11x - 14$.

Proof: Since 7 divides $3x+2$, we know that $3x+2 = 7a$, where a is _____. Notice that

$$15x^2 - 11x - 14 = (\_\_\_\_\_)(\_\_\_\_\_)$$

$$= \_\_\_\_\_a(5x - 7).$$

Therefore _____. □

Example 2.14. Let a and b be integers such that $a|b$ and $b|a$. Prove that either $a = b$ or $a = -b$.

Proof: If $a|b$, we can write $b = ac$ for some integer c. Similarly, if $b|a$, we can write $a = bd$ for some integer d. Then we can write $b = ac = (bd)c$. Dividing both sides by b (which is legal, since $b|a$ implies $b \neq 0$), we can see that $cd = 1$. Since c and d are integers, we know that either $c = d = 1$ or $c = d = -1$. In the first case, we have that $a = b$, and in the second case, we have that $a = -b$. □

★**Evaluate 2.15.** Prove that if n is an integer, then $n^3 - n$ is divisible by 6.

Proof: We have $n^3 - n = (n-1)n(n+1)$, the product of three consecutive integers. Among three consecutive integers at least one is even and exactly one is divisible by 3. Since 2 and 3 do not have common factors, 6 divides the quantity $(n-1)n(n+1)$, and so $n^3 - n$ is divisible by 6. □

Evaluation _____

Definition 2.16. *A positive integer $p > 1$ is* **prime** *if its only positive factors are 1 and p. A positive integer $c > 1$ which is not prime is said to be* **composite**.

★**Evaluate 2.17.** Prove or disprove that if a is a positive even integer, then it is composite.

Proof: Let a be an even number. By definition of even, $a = 2k$ for some integer k. Since $a > 0$, clearly $k > 0$. Since a has at least two factors, 2 and k, a is composite. □

Evaluation _____

_____

Note: *Notice that according to the definitions given above, 1 is neither prime nor composite. This is one of the many things that makes 1 special.*

★**Exercise 2.18.** Prove that 2 is the only even prime number.

Proof _____

_____

_____

★**Question 2.19.** Did you notice that the proof in the solution to the previous exercise (you read it, right?) did not consider the case of 0 or negative even numbers. Was that O.K.? Explain why or why not.

Answer _____

Definition 2.20. *For a non-negative integer n, the quantity $n!$ (read "n* **factorial**"*) is defined as follows. $0! = 1$ and if $n > 0$ then $n!$ is the product of all the integers from 1 to n inclusive:*

$$n! = 1 \cdot 2 \cdots n.$$

Example 2.21. $3! = 1 \cdot 2 \cdot 3 = 6$, and $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

Example 2.22. Prove that if $n > 0$, then $n! \leq n^n$.

Proof: Since $1 \leq n$, $2 \leq n$, $\cdots$, and $(n-1) \leq n$, it is easy to see that

$$\begin{aligned} n! &= 1 \cdot 2 \cdot 3 \cdots n \\ &\leq n \cdot n \cdot n \cdots n \\ &= n^n. \end{aligned}$$

□

★**Evaluate 2.23.** Prove that if $n > 4$ is composite, then n divides $(n-1)!$.

Proof: Since n is composite, n = ab for some integers 1 < a < n − 1 and 1 < b < n − 1. By definition of factorial, a|(n − 1)! and b|(n − 1)! Therefore n = ab divides (n − 1)! □

Evaluation _____

_____

Since the previous proof wasn't correct, let's fix it.

Example 2.24. Prove that if $n > 4$ is composite, then n divides $(n-1)!$.

Proof: If n is not a perfect square, then we can write $n = ab$ for some integers a and b with $1 < a < b < n-1$. Thus, $(n-1)! = 1 \cdots a \cdots b \cdots (n-1)$. Since a and b are distinct numbers on the factor list, $n = ab$ is clearly a factor of $(n-1)!$.

If n is a perfect square, then $n = a^2$ for some integer $2 < a < n-1$. Since $a > 2$, $2a < a^2 = n$. Thus, $2a < n$, so $(n-1)! = 1 \cdots a \cdots 2a \cdots (n-1)$. Then $a(2a) = 2n$ is a factor of $(n-1)!$, which means that n is as well. □

★**Question 2.25.** Why was it O.K. to assume $1 < a < b < n-1$ in the previous proof?

Answer _____

_____

_____

★**Question 2.26.** In the second part of the previous proof, why could we say that $a > 2$?

Answer _____

Example 2.27. Prove the *Arithmetic Mean-Geometric Mean Inequality*, which states that for all non-negative real numbers x and y,

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

Proof: Since x and y are non-negative, $\sqrt{x}$ and $\sqrt{y}$ are real numbers, so $\sqrt{x}-\sqrt{y}$ is a real number. Since the square of any real number is greater than or equal to 0 we have

$$(\sqrt{x}-\sqrt{y})^2 \geq 0.$$

Expanding (recall the FOIL method?) we get

$$x - 2\sqrt{xy} + y \geq 0.$$

Adding $2\sqrt{xy}$ to both sides and dividing by 2, we get

$$\frac{x+y}{2} \geq \sqrt{xy},$$

yielding the result. □

The previous example illustrates the creative part of writing proofs. The proof started out considering $\sqrt{x}-\sqrt{y}$, which doesn't seem to be related to what we wanted to prove. But hopefully after you read the entire proof you see why it makes sense. If you are saying to yourself "I would never have thought of starting with $\sqrt{x}-\sqrt{y}$?," or "How do you know where to start?," I am afraid there are no easy answers. Writing proofs is as much of an art as it is a science. There are three things that can help, though. First, *don't be afraid to* ***experiment***. If you aren't sure where to begin, try starting at the end. Think about the end goal and work backwards until you see a connection. Sometimes working both backward and forward can help. Try some algebra and see where it gets you. But in the end, make sure your proof goes from beginning to end. In other words, the order that you figured things out should not necessarily dictate the order they appear in your proof.

The second thing you can do is to ***read example proofs***. Although there is some creativity necessary in proof writing, it is important to follow proper proof writing techniques. Although there are often many ways to prove the same statement, there is often one technique that works best for a given type of problem. As you read more proofs, you will begin to have a better understanding of the various techniques used, know when a particular technique might be the best choice, and become better at writing your own proofs. If you see several proofs of similar problems, and the proofs look very similar, then when you prove a similar problem, your proof should probably resemble those proofs. This is one area where some students struggle—they submit proofs that look nothing like any of the examples they have seen, and they are often incorrect. Perhaps it is because they are afraid that they are plagiarizing if they mimic another proof too closely. However, mimicking a proof is not the same as plagiarizing a sentence. To be clear, by 'mimic', I don't mean just copy exactly what you see. I mean that you should read and understand several examples. Once you understand the technique used in those examples, you should be able to see how to use the same technique in your proof. For instance, in many of the examples related to even numbers, you may have noticed that they start with statement like *"Assume x is even. Then $x = 2a$ for some integer a."* So if you need to write a proof related to even numbers, what sort of statement might make sense to begin your proof?

The third thing that can help is ***practice***. This applies not only to writing proofs, but to learning many topics. An analogy might help here. Learning is often like sports—you don't learn how to play basketball (or insert your favorite sport, video game, or other hobby that takes some skill) by reading books and/or watching people play it. Those things can be helpful (and in some cases necessary), but you will never become a proficient basketball player unless you practice. Practicing a sport involves running many drills to work on the fundamentals and then applying

the skills you learned to new situations. Learning many topics is exactly the same. First you need to do lots of exercises to practice the fundamental skills. Then you can apply those skills to new situations. When you can do that well, you know you have a good understanding of the topic. So if you want to become better at writing proofs, you need to write more proofs.

★**Question 2.28.** What three things can help you learn to write proofs?

1. _____

2. _____

3. _____

2.2 Implication and Its Friends

This section is devoted to developing some of the concepts that will be necessary for us to discuss the ideas behind the next few proof techniques.

Although not technically interchangeable, you may sometimes see the word *statement* instead of *proposition*. Context should help you determine whether or not a given usage of the word *statement* should be understood to mean *proposition*. We saw the following in the previous chapter, but it is worth giving the definition again (stated slightly differently here so it better fits with our usage in this context).

Definition 2.29. *An* **implication** *is a proposition of the form "if p, then q," where p and q are propositions. p is called the* **premise** *and q is called the* **conclusion**.

It is sometimes written as $p \to q$, which is read "p implies q." It is a statement that asserts that if p is a true proposition then q is a true proposition.

An implication is true unless p is true and q is false.

Example 2.30. The proposition "If I do well in this course, then I can take the next course" is an implication. However, the proposition "I can do well in this course and take the next course" is *not* an implication.

Example 2.31. Consider the implication

"If you read *xkcd*, then you will laugh."[a]

If you read *xkcd* and laugh, you are being consistent with the proposition. If you read *xkcd* and *do not laugh*, then you are demonstrating that the proposition is false.

But what if you don't read *xkcd*? Are you demonstrating that the proposition is true or false? Does it matter whether or not you laugh? It turns out that you are *not* disproving it in this case–in other words, the proposition is still true if you don't read *xkcd*, whether or not you laugh. Why? Because the statement is not saying anything about laughing by itself. It is only asserting that ***IF*** you read *xkcd*, then you will laugh. In other words, it is a *conditional statement*, with the condition being that you read *xkcd*. The statement is saying nothing about anything if you don't read *xkcd*.

So the bottom line is that if you do not read *xkcd*, the statement is still true.

[a] If you are unfamiliar with *xkcd*, go to http://xkcd.com, but don't get distracted for too long!

★**Question 2.32.** When is the implication "If you read *xkcd*, then you will laugh" false?

Answer _____

_____

★**Exercise 2.33.** Consider the implication "If you build it, they will come." What are all of the possible ways this proposition could be false?

Solution _____

_____

_____

Given an implication $p \to q$, there are three related propositions. We will introduce each and discuss how they are related to each other.

Definition 2.34. *The* **contrapositive** *of a proposition of the form "if p, then q" is the proposition "if q is not true, then p is not true" or "if not q, then not p" or* $\neg q \to \neg p$.

★**Question 2.35.** What is the contrapositive of the proposition "If you know Java, then you know a programming language"?

Answer _____

_____

Theorem 2.36. *An implication is true if and only if its contrapositive is true. Stated another way,* **an implication and its contrapositive are equivalent**.

★**Fill in the details 2.37.** Prove Theorem 2.36.

Proof: Let $p \to q$ be our implication. According to the definition of implication, it is false when p is true and q is false and _____ otherwise. Put another way, it is true unless p is true and q is false. The contrapositive, $\neg q \to \neg p$, is false when $\neg q$ is true and _____ is false, and true otherwise. Notice that this is equivalent to q being _____ and _____ being true. Thus, the contrapositive is true unless _____ and _____. But this is exactly when $p \to q$ is true. □

Definition 2.38. *The* **inverse** *of a proposition of the form "if p, then q" is the proposition "if p is not true, then q is not true" or "if not p, then not q" or* $\neg p \to \neg q$.

★**Question 2.39.** What is the inverse of the proposition "If you know Java, then you know a programming language"?

Answer _____

★**Question 2.40.** Are a proposition and its inverse equivalent? Explain, using the proposition from Question 2.39 as an example.

Answer _____

_____

_____

Definition 2.41. *The* **converse** *of a proposition of the form "if p, then q" is the proposition "if q, then p" or $q \to p$.*

★**Question 2.42.** What is the converse of the proposition "If you know Java, then you know a programming language"?

Answer _____

★**Question 2.43.** Are a proposition and its converse equivalent? Explain using the proposition about Java/programming languages.

Answer _____

_____

_____

As you have just seen, the *inverse* and *converse* of an implication are not equivalent to the implication. However, it turns out that the *inverse* and *converse* of a proposition are equivalent to each other.

Theorem 2.44. *The inverse of an implication is true if and only if the converse of the implication is true. Stated another way,* **the inverse and converse of an implication are equivalent to each other**.

You will be asked to prove Theorem 2.44 in Problem 2.2. If you think about it in the right way, it should be fairly easy to prove. Table 2.1 summarizes what we know.

Implication Contrapositive	$p \to q$ $\neg q \to \neg p$	}	Equivalent
Converse Inverse	$q \to p$ $\neg p \to \neg q$	}	Equivalent

Table 2.1: Implication and friends

Example 2.45. Here is an example of an implication and its friends:

1. **Implication** If I get to watch "The Army of Darkness," then I will be happy.
2. **Inverse** If I do not get to watch "The Army of Darkness," then I will not be happy.
3. **Converse** If I am happy, then I got to watch "The Army of Darkness."
4. **Contrapositive** If I am not happy, then I didn't get to watch "The Army of Darkness."

★**Question 2.46.** Using the propositions from the previous example, answer the following questions.

(a) Give an explanation of why an *implication* might be true, but the *inverse* false.

Answer _____

_____

_____

(b) Explain why an *implication* is saying the exact same thing as its *contrapositive*. (Don't just say "By Theorem 2.36.")

Answer _____

_____

_____

Implications can be tricky to fully grasp and it is easy to get your head turned around when dealing with them. We will discuss them in quite a bit of detail throughout the next few sections in order to help you understand them better.

2.3 Proof by Contradiction

In this section we will see examples of *proof by contradiction*. For this technique, when trying to prove a statement, we assume that its negation is true and deduce incompatible statements from this (i.e. we prove something we know to be false). This implies that the original statement must be true.

When applied to a proposition, we assume that the premise is true but the conclusion is false, with the goal still to show that something that is false is true. Since we "obtained a contradiction," it must be that the conclusion is true. We will explain in more detail the idea behind this proof technique after a few examples.

Example 2.47. Prove that if $5n + 2$ is odd, then n is odd.

> **Proof:** Assume that $5n + 2$ is odd, but that n is even. Then $n = 2k$ for some integer k. This implies that $5n + 2 = 5(2k) + 2 = 10k + 2 = 2(5k + 1)$, which is even. But this contradicts our assumption that $5n + 2$ is odd. Therefore it must be the case that n is odd. □

The idea behind this proof is that if we are given the fact that $5n + 2$ is odd, we are asserting that n must be odd. How do we prove that n is odd? We could try a direct proof, but it is actually easier to use a proof by contradiction in this case. The idea is to consider what would happen if n is *not* odd. What we showed was that if n is not odd, then $5n + 2$ has to be even. But we *know* that $5n + 2$ is odd because that was our initial assumption. How can $5n + 2$ be both odd and even? It can't. In other words, our proof lead to a contradiction–an impossibility. Therefore, something is wrong with the proof. But what? If n is indeed even, our proof that $5n + 2$ is even is correct. So there is only one possible problem–n must not be even. The only alternative is that n is odd. Can you see how this proves the statement "if $5n + 2$ is odd, then n is odd?"

Note: *If you are somewhat confused at this point that's probably O.K. Keep reading, and re-read this section a few times if necessary. At some point you will have an "Aha" moment and the idea of contradiction proofs will make sense.*

Example 2.48. Prove that if $n = ab$, where a and b are positive integers, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

> **Proof:** Let's assume that $n = ab$ but that the statement "either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" is false. Then it must be the case that $a > \sqrt{n}$ and $b > \sqrt{n}$. But then $ab > \sqrt{n}\sqrt{n} = n$. But this contradicts the fact that $ab = n$. Since our assumption that $a > \sqrt{n}$ and $b > \sqrt{n}$ lead to a contradiction, it must be false. Therefore it must be the case that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. □

Sometimes your proofs will not directly contradict an assumption made but instead will contradict a statement that you otherwise know to be true. For instance, if you ever conclude that $0 > 1$, that is a contradiction. The next example illustrates this.

★**Fill in the details 2.49.** Show, without using a calculator, that $6 - \sqrt{35} < \frac{1}{10}$.

Proof: Assume that $6 - \sqrt{35} \geq \frac{1}{10}$. Then $6 - \frac{1}{10} \geq$_____. If we multiple both sides by 10 and do a little arithmetic, we can see that $59 \geq$_____ .

Squaring both sides we obtain _____, which is clearly _____.

Thus it must be the case that $6 - \sqrt{35} < \frac{1}{10}$. □

Now that we have seen a few examples, let's discuss contradiction proofs a little more formally. Here is the basic concept of contradiction proofs: You want to prove that a statement p is true. You "test the waters" by seeing what happens if p is *not* true. So you assume p is false and use proper proof techniques to arrive at a contradiction. By "contradiction" I mean something that cannot possibly be true. Since you proved something that is not true, and you used proper proof techniques, then it must be that your assumption was incorrect. Therefore the negation of your assumption—which is the original statement you wanted to prove—must be true.

★**Evaluate 2.50.** Use the definition of even and odd to prove that if a and b are integers and ab is even, then at least one of a or b is even.

Proof 1: By definition of even numbers, let a be an even integer 2n, and by the definition of odd numbers, let b be an odd integer 2q + 1. Then (2n)(2q + 1) = 4nq + 2n = 2(2nq + 1). Since 2nq + 1 is an integer, 2(2nq + 1) is an even integer by definition of even.

Evaluation _____

Proof 2: If true, either one is odd and the other even, or they are both even, so we will show that the product of an even and an odd is even, and that the product of two evens integers is even.
Let a = 2k and b = 2x + 1. (2k)(2x + 1) = 4kx + 2k = 2(2kx + k). 2kx + k is an integer so 2(2kx + k) is even.
Let a = 2k and b = 2x. (2k)(2x) = 4kx = 2(2kx) since 2kx is an integer, 2(2kx) is even.
Thus, if a and b are integers, ab is even, at least one of a or b is even.

Evaluation _____

Proof 3: Let a and b be integers and assume that ab is even, but that neither a nor b is even. Then both a and b are odd, so $a = 2n+1$ and $b = 2m+1$ for some integers n and m. But then $ab = (2n+1)(2m+1) = 4nm+2n+2m+1 = 2(2nm+n+m)+1$, which is odd since $2nm+n+m$ is an integer. This contradicts the fact that ab is even. Therefore either a or b must be even.

Evaluation _____

_____

_____

For some students, the trickiest part of contradiction proofs is what to contradict. Sometimes the contradiction is the fact that p is true. At other times you arrive at a statement that is clearly false (e.g. $0 > 1$). Generally speaking, you should just try a few things (e.g. do some algebra) and see where it leads. With practice, this gets easier. In fact, with enough practice this will probably become one of your favorite techniques. When a direct proof doesn't seem to be working this is usually the next technique I try.

Example 2.51. Let a_1, a_2, ..., a_n be real numbers. Prove that at least one of these numbers is greater or equal to the average of the numbers.

Proof: The average of the numbers is $A = (a_1+a_2+\ldots+a_n)/n$. Assume that none of these numbers is greater than or equal to A. That is, $a_i < A$ for all $i = 1, 2, \ldots n$. Thus $(a_1+a_2+\ldots+a_n) < nA$. Solving for A, we get $A > (a_1+a_2+\ldots+a_n)/n = A$, which is a contradiction. Therefore at least one of the numbers is greater than or equal to the average. □

Our next contradiction proof involves *permutations*. Here is the definition and an example in case you haven't seen these before.

Definition 2.52. *A* **permutation** *is a function from a finite set to itself that reorders the elements of the set. Since we haven't formally discussed functions yet, the following informal definition will probably make more sense to some of you: a* **permutation** *of a set of objects is an ordering of those objects.*

Example 2.53. Let S be the set $\{a, b, c\}$. Then (a, b, c), (b, c, a) and (a, c, b) are permutations of S. (a, a, c) is not a permutation of S because it repeats a and does not contain b. (b, d, a) is not permutations of S because d is not in S, and c is missing.

★**Exercise 2.54.** List all of the permutations of the set $\{1, 2, 3\}$. (Hint: There are 6.)

Answer _____

_____

Note: *In many contexts, when a list of objects occurs in* **curly braces**, *the order they are listed does not matter (e.g.* $\{a, b, c\}$ *and* $\{b, c, a\}$ *mean the same thing). On the other hand, when a list occurs in* **parentheses**, *the order* **does** *matter. Thus,* (a, b, c) *and* (b, c, a) **do not** *mean the same thing.*

Example 2.55. Let $(a_1, a_2, \ldots, a_n)$ be an arbitrary permutation of the numbers $1, 2, \ldots, n$, where n is an odd number. Prove that the product $(a_1 - 1)(a_2 - 2) \cdots (a_n - n)$ is even.

> **Proof:** Assume that the product is odd. Then all of the differences $a_k - k$ must be odd. Now consider the sum $S = (a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n)$. Since the a_k's are a just a reordering of $1, 2, \ldots, n$, $S = 0$. But S is the sum of an odd number of odd integers, so it must be odd. Since 0 is not odd, we have a contradiction. Thus our initial assumption that all of the $a_k - k$ are odd is wrong, so at least one of them is even and hence the product is even. □

★**Question 2.56.** Why did the previous proof begin by assuming that the product was odd?

Answer _____

_____

_____

★**Question 2.57.** In the previous proof, we asserted that $S = 0$. Why was this the case?

Answer _____

_____

_____

We will use facts about rational/irrational numbers to demonstrate some of the proof techniques. In case you have forgotten, here are the definitions.

Definition 2.58. *Recall that*

- *A* **rational number** *is one that can be written as* p/q, *where* p *and* q *are integers, with* $q \neq 0$.
- *An* **irrational number** *is a real number that is not rational.*

Example 2.59. Prove that $\sqrt{2}$ is irrational. We present two slightly different proofs. In both, we will use the fact that any positive integer greater than 1 can be factored uniquely as the product of primes (up to the order of the factors).

Proof 1: Assume that $\sqrt{2} = \frac{a}{b}$, where a and b are positive integers with $b \neq 0$. We can assume a and b have no factors in common (since if they did, we could cancel them and use the resulting numerator and denominator as a and b). Multiplying by b and squaring both sides yields $2b^2 = a^2$. Clearly 2 must be a factor of a^2. Since 2 is prime, a must have 2 as a factor, and therefore a^2 has 2^2 as a factor. Then $2b^2$ must also have 2^2 as a factor. But this implies that 2 is a factor of b^2, and therefore a factor of b. This contradicts the fact that a and b have no factors in common. Therefore $\sqrt{2}$ must be irrational.

Proof 2: Assume that $\sqrt{2} = \frac{a}{b}$, where a and b are positive integers with $b \neq 0$. Multiplying by b and squaring both sides yields $2b^2 = a^2$. Now both a^2 and b^2 have an even number of prime factors. So $2b^2$ has an odd number of primes in its factorization and a^2 has an even number of primes in its factorization. This is a contradiction since they are the same number. Therefore $\sqrt{2}$ must be irrational.

★**Question 2.60.** In proof 2 from the previous example, why do a^2 and b^2 have an even number of factors?

Answer _____

_____

_____

Now that you have seen a few more examples, it is time to begin the discussion about how/why contradiction proofs work. We will start with the following idea that you may not have thought of before. It turns out that if you start with a false assumption, then you can prove that *anything* is true. It may not be obvious how (e.g. How would you prove that all elephants are less than 1 foot tall given that $1 + 1 = 1$?), but in theory it is possible. This is because statements of the form "p implies q" are true if p (called the *premise*) is false, regardless of whether or not q (called the *conclusion*) is true or false.

Example 2.61. The statement "If chairs and tables are the same thing, then the moon is made of cheese" is true. This may seem weird, but it is correct. Since chairs and tables are not the same thing, the premise is false so the statement is true. But it is important to realize that the fact that the whole statement is true doesn't tell us anything about whether or not the moon is made of cheese. All we know is that *if* chairs and tables were the same thing, then the moon *would have to* be made out of cheese in order for the statement to be true.

Example 2.62. Consider what happens if your parents tell you "If you clean your room, then we will take you to get ice cream." If you don't clean your room and your parents don't take you for ice cream, did your parents tell a lie? No. What if they *do* take you for ice cream? They still haven't lied because they didn't say they wouldn't take you if you didn't clean your room. In other words, if the premise is false, the whole statement is true regardless of whether or not the conclusion is true.

It is important to understand that when we say that a statement of the form "p implies q" is true, we are *not* saying that q is true. We are only saying that *if p is true, then q has to be true.*

We aren't saying anything about q by itself. So, if we know that "p implies q" is true, and we also know that p is true, then q must also be true. This is a rule called *modus ponens*, and it is at the heart of contradiction proofs as we will see shortly.

★**Exercise 2.63.** It might help to think of statements of the form "p implies q" as rules where breaking them is equivalent to the statement being false. For instance, consider the statement *"If you drink alcohol, you must be 21."* If we let p be the statement "you drink alcohol" and q be the statement "you are 21," the original statement is equivalent to "p implies q".

1. If you drink alcohol and you are 21, did you break the rule? _____
2. If you drink alcohol and you are not 21, did you break the rule? _____
3. If you do not drink alcohol and you are 21, did you break the rule? _____
4. If you do not drink alcohol and you are not 21, did you break the rule? _____
5. Generalize the idea. If you have a statement of the form "p implies q", where p and q can be either true or false statements, exactly when can the statement be false?

   _____
6. If you do not drink alcohol, does it matter how old you are? _____
7. Can a statement of the form "p implies q" be false if p is false? Explain.

   _____

   _____

Now we are ready to explain the idea behind contradiction proofs. We want to prove some statement p is true. We begin by assuming it is false—that is, we assume $\neg p$ is true. We use this fact to prove that q—some false statement—is true. In other words, we prove that the statement "$\neg p$ implies q" is true, where q is some false statement. But if $\neg p$ is true, and "$\neg p$ implies q" is true, modus ponens tells us that q is true. Since we know that q is false, something is wrong. We only have two choices: either $\neg p$ is false or "$\neg p$ implies q" is false. If we used proper proof techniques to establish that "$\neg p$ implies q" is true, then that isn't the problem. Therefore, $\neg p$ must be false, implying that p is true. That is why contradiction proofs work.

Let's analyze the second proof from Example 2.59 in light of this discussion. The *only* assumption we made was that $\sqrt{2}$ is rational ($\neg p$="$\sqrt{2}$ is rational"). From this (and only this), we were able to show that a^2 has both an even and an odd number of factors (q="a^2 has an even and an odd number of factors", and we showed that "$\neg p$ implies q" is true). Thus, we know for certain that if $\sqrt{2}$ is rational, then a^2 has an even and an odd number of factors.[1] This fact is indisputable since we proved it. If it is also true that $\sqrt{2}$ is rational, modus ponens implies that a^2 has an even and an

[1]We did not prove that a^2 has an even and an odd number of factors. We proved that *if* $\sqrt{2}$ *is rational*, then a^2 has an even and an odd number of factors. It is very important that you understand the difference between these two statements.

odd number of factors. This is also indisputable. But we know that a^2 cannot have both an even and odd number of factors. In other words, we have a contradiction. Therefore, something that has been said somewhere is wrong. Everything we said is indisputable except for one thing–that $\sqrt{2}$ is rational. That was never something we proved—we just assumed it. So it has to be the case that this is false, which means that $\sqrt{2}$ must be irrational.

To summarize, if you want to prove that a statement is true using a contradiction proof, assume the statement is false, use this assumption to get a contradiction (i.e. prove a false statement), and declare that it must therefore be true.

Notice that what q is doesn't matter. In other words, given the assumption $\neg p$, the goal in a contradiction proof is to establish that *any* false statement is true. This is both a blessing and a curse. The blessing is that any contradiction will do. The curse is that we don't have a clear goal in mind, so it can sometimes be difficult to know what to do. As mentioned previously, this becomes easier as you read and write more proofs.

If this discussion has been a bit confusing, try re-reading it. The better you understand the theory behind contradiction proofs, the better you will be at writing them. We will revisit some of these concepts in the chapter on logic, so the more you understand from here, the better off you will be when you get there. O.K., enough theory. Let's see some more examples!

★**Fill in the details 2.64.** Let a, b be real numbers. Prove that if $a < b + \epsilon$ for all $\epsilon > 0$, then $a \leq b$.

Proof: We will prove this by contradiction. Assume that _____.[a] Subtracting b from both sides and dividing by 2, we get _____ > 0. Since the inequality $a < b+\epsilon$ holds for every $\epsilon > 0$ in particular it holds for $\epsilon =$_____.[b] This implies that

$$a < b + \frac{a-b}{2} = \text{\_\_\_\_\_}.$$

If we _____ (to the previous equation), we obtain $a < b$. But we started with the assumption that _____ which is a _____. Therefore, _____. □

[a] Hint: What assumption do we always make when doing a contradiction proof?
[b] Same as the previous blank

The following beautiful proof goes back to Euclid. It uses the assumption that any integer greater than 1 is either a prime or a product of primes.

Example 2.65 (Euclid)**.** Show that there are infinitely many prime numbers.

Proof: Assume that there are only a finite number of primes and label the primes

$\{p_1, p_2, \ldots, p_n\}$. Consider the number

$$N = p_1 p_2 \cdots p_n + 1.$$

This is a positive integer that is clearly greater than 1. Observe that none of the primes on the list $\{p_1, p_2, \ldots, p_n\}$ divides N, since division by any of these primes leaves a remainder of 1. Since N is larger than any of the primes on this list, it is either a prime or divisible by a prime outside this list. But we assumed the list above contained all of the prime numbers. This is a contradiction. Therefore there must be infinitely many primes. □

★**Fill in the details 2.66.** If a, b, c are odd integers, prove that $ax^2 + bx + c = 0$ does not have a rational number solution.

Proof: Suppose $\frac{p}{q}$ is a rational solution to the equation. We may assume that p and q have no prime factors in common, so either p and q are both odd, or one is odd and the other even. Since $\frac{p}{q}$ is a solution, we know that

_____ $= 0$.

If we _____, we obtain $ap^2 + bpq + cq^2 = 0$.

If both p and q are odd, then $ap^2 + bpq + cq^2$ is _____ which contradicts the fact that it is _____.

If p is even and q odd, then _____

_____.

If p is odd and q even, then _____

_____.

Since all possibilities leads to a contradiction, _____.

_____

□

One final note on contradiction proofs: Only use one when you really need it. If a direct proof will work, use it. If you use a contradiction proof instead, you will just be making the proof more complicated for no good reason. Some students seem to grab onto contradiction proofs and try to use it for everything, but they are not the best choice in many cases.

2.4 Proof by Contraposition

Consider the statement "If it rains, then the ground will get wet." It should be pretty easy to convince yourself that this is essentially equivalent to the statement "If the ground is not wet, then it didn't rain." In fact, since the second statement is just the contrapositive of the first, Theorem 2.36 tells us that they are equivalent. Again, by *equivalent* we simply mean that either both statements are true or both statements are false. This is the idea behind the proof technique in this section.

Definition 2.67. *A* **proof by contraposition** *is a proof of a statement of the form "if p, then q" that proves contrapositive statement instead. That is, it proves the equivalent statement "if not q, then not p."*

Example 2.68. Prove that if $5n + 2$ is odd, then n is odd.

Proof: We will instead prove that if n is even (not odd), then $5n+2$ is even (not odd). Since this is the contrapositive of the original statement, a proof of this will prove that that the original statement is true.

Assume n is even. The $n = 2a$ for some integer a. Then $5n + 2 = 5(2a) + 2 = 2(5a + 1)$. Since $5a + 1$ is an integer, $2(5a + 1)$ is even. □

Be careful with proof by contraposition. Do not make the mistake of trying to prove the *converse* or *inverse* instead of the *contrapositive*. In that case, you may (sometimes) write a correct proof, but it would be a proof of the wrong thing.

In the next example we will see the similarities and differences between contradiction proofs and proofs by contraposition.

Example 2.69. Prove that if $5n + 2$ is even, then n is even.

Proof by contraposition:
We will prove the equivalent statement that if n is odd, then $5n + 2$ is odd. Assume n is odd. Then $n = 2k + 1$ for some integer k. Then we have that

$$\begin{aligned} 5n + 2 &= 5(2k + 1) + 2 \\ &= 10k + 5 + 2 \\ &= 10k + 7 \\ &= 2(5k + 3) + 1 \end{aligned}$$

Since $5k+3$ is an integer, this shows that $5n + 2$ is odd.

Proof by contradiction:
Assume that $5n+2$ is even but that n is odd. Since n is odd, $n = 2k+1$ for some integer k. Therefore

$$\begin{aligned} 5n + 2 &= 5(2k + 1) + 2 \\ &= 10k + 5 + 2 \\ &= 10k + 7 \\ &= 2(5k + 3) + 1 \end{aligned}$$

which is odd since $5k + 3$ is an integer. But we assumed that $5n + 2$ was even, which is a contradiction. Therefore our assumption that n is odd must be incorrect, so n is even.

★**Evaluate 2.70.** Let n be an integer. Use the definition of even/odd to prove that if $3n + 2$ is even, then n is even using a proof by contraposition.

Proof 1: We need to show that if n is even, then 3n + 2 is even. If n is even, then n = 2k for some integer k. Then 3n + 2 = 3(2k + 2) = 6k + 6 = 2(3k) + 2(3), which is even because it is the sum of two even integers.

Evaluation _____

Proof 2: We need to show that if n is odd, then 3n + 2 is odd. If n is odd then n = 2k + 1 for some integer k. Then 3n + 2 = 3(2k + 1) + 2 = 6k + 3 + 2 = 6k + 5 = 5($\frac{6}{5}$k + 1), which is clearly odd.

Evaluation _____

Proof 3: We need to show that if n is odd, then 3n + 2 is odd. If n is odd then n = 2k + 1 for some integer k. Then 3n + 2 = 3(2k + 1) + 2 = 6k + 5, which is odd by the definition of odd.

Evaluation _____

2.5 Other Proof Techniques

There are many other proof techniques. We conclude this chapter with a small sampling of the more common and/or interesting ones. We will see a few other important proof techniques later in the book.

Definition 2.71. *A* **trivial proof** *is a proof of a statement of the form "if p, then q" that doesn't use p in the proof.*

Example 2.72. Prove that if $x > 0$, then $(x+1)^2 - 2x > x^2$.

Proof: It is easy to see that

$$\begin{aligned}(x+1)^2 - 2x &= (x^2 + 2x + 1) - 2x \\ &= x^2 + 1 \\ &> x^2.\end{aligned}$$

Notice that we never used the fact that $x > 0$ in the proof. □

Definition 2.73. *A* **proof by counterexample** *is used to disprove a statement by giving an example of it being false.*

Example 2.74. Prove or disprove that the product of two irrational numbers is irrational.

Proof: We showed in Example 2.59 that $\sqrt{2}$ is irrational. But $\sqrt{2} * \sqrt{2} = 2$, which is an integer so it is clearly rational. Thus the product of 2 irrational number is not always irrational. □

Example 2.75. Prove or disprove that "Everybody Loves Raymond" (or that "Everybody Hates Chris").

Proof: Since I don't really love Raymond (I also don't hate Chris, in case you care), the statement is clearly false. □

★**Exercise 2.76.** Prove or disprove that the sum of any two primes is also prime.

Proof _____

_____

_____

Definition 2.77. *A* **proof by cases** *breaks up a statement into multiple cases and proves each one separately.*

We have already seen several examples of proof by cases (e.g. Examples 2.24 and 2.66), but it never hurts to see another example.

Example 2.78. Prove that if $x \neq 0$ is a real number, then $x^2 > 0$.

Proof: If $x \neq 0$, then either $x > 0$ or $x < 0$.

If $x > 0$ (case 1), then we can multiply both sides of $x > 0$ by x, giving $x^2 > 0$.

If $x < 0$ (case 2), then we can write y=-x, where $y > 0$. Then $x^2 = (-y)^2 = (-1)^2 y^2 = y^2 > 0$ by case 1 (since $y > 0$). Thus $x^2 > 0$. In either case, we have shown that $x^2 > 0$. □

★**Fill in the details 2.79.** Let s be a positive integer. Prove that the closed interval $[s, 2s]$ contains a power of 2.

Proof: If s is a power of 2 then _____

If s is not a power of 2, then it is strictly between two powers of 2. That is,

$2^{r-1} < s < 2^r$ for some integer r. Then _____

_____

_____

□

2.6 If and Only If Proofs

Sometimes we will run into "if and only if" (abbreviated *iff*) statements. That is, statements of the form p **if and only if** q. This is equivalent to the statement "p implies q and q implies p." Thus, to prove that an iff statement is true, you need to prove a statement and its *converse*. "p implies q" is sometimes called the *forward direction* and the converse is sometimes called the *backwards direction*. Sometimes the converse statement is proven by *contraposition*, so that instead of proving q implies p, $\neg p$ implies $\neg q$ is proven.

★**Question 2.80.** Why is there a choice between proving q **implies** p and proving $\neg p$ **implies** $\neg q$ when proving the backwards direction?

Answer _____

_____

Example 2.81. Prove that x is even if and only if $x + 10$ is even.

Proof: If x is even, then $x = 2k$ for some integer k. Then $x + 10 = 2k + 10 = 2(k + 5)$. Since $k + 5$ is an integer, then $x + 10$ is even. Conversely, if $x + 10$ is even, then $x + 10 = 2k$ for some integer k. Then $x = (x + 10) - 10 = 2k - 10 = 2(k - 5)$. Since $k - 5$ is an integer, then x is even. Therefore x is even iff $x + 10$ is even. □

As we have mentioned before, the examples in this section are quite trivial and may seem ridiculous–since they are so obvious, why are we bothering to prove them? The point is to use the proof techniques we are learning. We will use the techniques on more complicated problems later. For now we want the focus to be on proper use of the techniques. That is more easily accomplished if you don't have to think too hard about the details of the proof.

★**Exercise 2.82.** Prove that x is odd iff $x + 20$ is odd using direct proofs for both directions

★**Exercise 2.83.** Prove that x is odd iff $x + 20$ is odd using using a direct proof for the forward direction and a proof by contraposition for the backward direction.

★**Fill in the details 2.84.** The two most common ways to prove p iff q are

1. Prove that _____ and _____, or
2. Prove that _____ and _____.

★**Evaluate 2.85.** Use the definition of odd to prove that x is odd if and only if $x - 4$ is odd.

Proof 1: Assume x is odd. Then $x = 2k+1$ for some integer k. Then $x-4 = 2k+1-4 = 2k-3$, which is odd. Now assume that $x-4$ is odd. Since $(2k+1)-4$ is odd, then $x = 2k+1$ is clearly odd.

Evaluation _____

Proof 2: Assume x is odd. Then $x = 2k+1$, so $x-4 = (2k+1)-4 = 2(k-2)+1$, which is odd since $k-2$ is an integer. Now assume $x-4$ is even. Then $x-4 = 2k$ for some integer k. Then $x = 2k+4 = 2(k+2)$, which is even since $k+2$ is an integer.

Evaluation _____

2.7 Common Errors in Proofs

If you arrive at the right conclusion, does that mean your proof is correct? Some students seem to think so, but this is absolutely false. Let's consider the following example.

Example 2.86. Is the following proof that $\frac{16}{64} = \frac{1}{4}$ correct? Why or why not?

Proof: This is true because if I cancel the 6 on the top and the bottom, I get $\frac{16}{64} = \frac{1\cancel{6}}{\cancel{6}4} = \frac{1}{4}$. □

Evaluation: You probably know that you can't cancel arbitrary digits in a fraction, so this is not a valid proof. In addition, consider this: If this proof is correct, then it could be used to prove that $\frac{16}{61} = \frac{1\cancel{0}}{\cancel{0}1} = \frac{1}{1} = 1$, which is clearly false.

Note: *The point of the previous example is this: Don't confuse the fact that what you are trying to prove is true with whether or not your proof actually* proves *that it is true. An incorrect proof of a correct statement is no proof at all.*

One rookie mistake that I see often is *proof by example*, where the writer attempts to prove something in general by proving it for one particular case and assuming it must therefore work for all of the other cases.

★**Question 2.87.** What is wrong with this 'proof' that the sum of two even integers is even?

Proof: Let x and y be even integers. Assume $x = 4$ and $y = 6$, which are both even. Then $x + y = 10 = 2 * 5$, which is even since 5 is an integer. Thus, the sum of two even integers is even. □

Answer _____

_____

Just because a proof seems work out, it does not mean that it is a proof of the correct statement. For instance, the proof in Question 2.87 is a correct proof of the fact that the sum of 4 and 6 is even. But it is certainly *not* a proof that the sum of *any* two even numbers is even.

Let's see an example of a supposed proof of something that is not even true. Hopefully I do not need to convince you that the proof cannot be valid (since the statement is false).

Example 2.88. What is wrong with this 'proof' that one more than an even number is divisible by 3?

Proof: Notice that $14 + 1 = 15 = 3 * 5$ which is clearly divisible by 3. Since $14 = 2 * 7$ is even, we just showed that one more than an even number is divisible by 3. □

Evaluation: This only shows that one more than 14 is divisible by 3. Notice that

10 is even, but $10+1 = 11$ is not divisible by 3, so the statement that is supposedly being proven here is clearly not true!

Hopefully this example helps you see the problem with *proof by example*. If the technique worked, then the proof in the previous example is a valid proof of the false statement that one more than an even number is divisible by 3. But since that statement is false, it can't have been a valid proof. Indeed, as we already mentioned, the proof does show that the statement is true for the given even number (in this case, 14), but that does not imply anything about the validity of the statement for any other even numbers.

If you want to prove something for a general collection of numbers (e.g. even number, integers, etc.), then your proof has to be general enough to include all possible values. For instance, if you want to prove something about odd numbers, then you let $x = 2k+1$ where k is an integer. Notice that no matter which odd integer you want to consider, you can pick k to obtain that value. Thus, if you prove something about the value $x = 2k + 1$, then you have proven it for all odd values of x. However, if you show it is true for $x = 7$ (for instance), you have only shown that it is true for $x = 7$.

Another common mistake when writing proofs is to make one or more invalid assumptions without realizing it. This is another case where you end up proving a different statement (usually a more specific statement) than the one you set out to prove. The problem is that when you make this sort of mistake, the proof can sometimes seems to "work" because you get the conclusion you want. Thus, your proof might actually be a valid proof, but it is of the wrong statement. Thus, it isn't always obvious that you even made a mistake.

The next few examples should illustrate what can go wrong if you aren't careful.

★**Question 2.89.** What is wrong with this 'proof' that the sum of two even integers is even?

Proof: Let x and y be even integers. Then $x = 2a$ for some integer a and $y = 2a$ for some integer a. So $x + y = 2a + 2a = 2(a + a)$. Since $a + a$ is an integer, $2(a + a)$ is even, so the sum of two even integers is even. □

Answer _____

_____

Since the statement in the previous example is true, it can be difficult to appreciate why the proof is wrong. The proof seems to prove the statement but as you saw in the solution, it actually doesn't. It proves a more specific statement (In this case, it is a proof of the fact that the sum of an even number with itself is even when it was supposed to be a proof of the fact that the sum of any two even numbers is even.).

If it seems like we are being too nit-picky, consider the next example which gives a supposed proof that the sum of two even numbers is divisible by 4 (hopefully you can quickly convince yourself that this is not a true statement).

★**Question 2.90.** What is wrong with the following 'proof' that the sum of two even integers is divisible by 4?

Proof: Let x and y be two even integers. Then $x = 2a$ for some integer a and $y = 2a$ for some integer a. So $x + y = 2a + 2a = 4a$. Since a is an integer, $4a$ is divisible by 4, so the sum of two even integers is divisible by 4. □

Answer _____

_____

Another common mistake students make when trying to prove an identity/equation is to start with what they want to prove and work both sides of it until they demonstrate that they are equal. I want to stress that *this is an invalid proof technique.* Again, if this seems like I am making something out of nothing, consider this example:

★**Question 2.91.** Consider the following supposed proof that $-1 = 1$.

Proof:

$$\begin{aligned} -1 &= 1 \\ (-1)^2 &= 1^2 \\ 1 &= 1 \end{aligned}$$

Therefore $-1 = 1$. □

How do you know that this proof is incorrect? (Think about the obvious reason, not any technical reason.)

Answer _____

Notice that each step of algebra in the previous proof is correct. For instance, if $a = b$, then $a^2 = b^2$ is correct. And $(-1)^2$ and 1^2 are both equal to 1. So the majority of the proof contains proper techniques. It contains just one problem: It starts by assuming something that isn't true. Unfortunately, one error is all it takes for a proof to be incorrect.

Note: *When writing proofs,* **never** *assume something that you don't already know to be true! In particular, if you are trying to prove an equality, never start with the equality and work both sides until you get the same thing. As demonstrated in the previous example, this is not a valid proof technique.*

★**Question 2.92.** When you are given an equation to prove, should you prove it by writing it down and working both sides until you get them both to be the same? Why or why not?

Answer _____

_____

Let's be clear about this issue. If you known an equation is correct, you can work both sides of it until you get to some desired conclusion. However, if you have an equation and you do not know whether or not it is correct, you cannot start your proof by considering that equation. As Example 2.91 demonstrated, if an equation is *not correct*, sometimes you can work both sides until they are the same, which gives the illusion that you have proven that it is correct, which is clearly not possible. Hopefully this makes it clear to you that beginning a proof with an unknown equation (e.g. the equation you are trying to prove) and using it in your proof is not valid.

★**Question 2.93.** You are given an equation. You work both sides of it until they are the same. Should you now be convinced that the equation is correct? Why or why not?

Answer _____

_____

Note: *If you already know that an equation is true, then working both sides of it (for some purpose other than demonstrating it is true)* is *a valid technique. However, it is more common to start with a known equation and work just one side until it is what we want.*

There are plenty of other common errors in proofs. We will see more examples of them throughout the remainder of the book (although we will focus more on correct proof techniques!), especially in the *Evaluate* examples. I want to say that you will likely see other examples of errors in proofs as you write your own proofs, but that would be mean. Probably accurate, but still mean.

2.8 More Practice

Now you will have a chance to practice what you have learned throughout this chapter with some more exercises. Now that they aren't in a particular section, you will have to figure out what technique to use.

★**Exercise 2.94.** Let $p < q$ be two *consecutive* odd primes (two primes with no other primes between them). Prove that $p + q$ is a composite number. Further, prove that it has at least three, not necessarily distinct, prime factors. (Hint: think about the average of p and q.)
Proof:

★**Evaluate 2.95.** Prove or disprove that if x and y are rational, then x^y is rational.

Proof 1: Because x and y are both rational, assume $x = a/b$ where a and b are integers and $b \neq 0$. We can assume that a and b have no factors in common (since if they did we could cancel them and use the resulting numbers as our new a and b). Then $x^y = \frac{a^y}{b^y}$, so x^y is rational.

Evaluation _____

Proof 2: Notice that x^y is just x multiplied by itself y times. A rational number multiplied by a rational number is rational, so x^y is rational.

Evaluation _____

Since none of the proofs in the previous example were correct, you need to prove it.

★**Exercise 2.96.** Prove or disprove that if x and y are rational, then x^y is rational.
Proof:

★**Evaluate 2.97.** Prove or disprove that if x is irrational, then $1/x$ is irrational.

Proof 1: If x is rational, assume it is an integer. If x is an integer, it is rational. 1/x is an integer over an integer, so it is rational. Therefore if x is rational, 1/x is rational, so by contrapositive reasoning, if x is irrational, 1/x is irrational.

Evaluation _____

Proof 2: Assume that x is irrational. Then it cannot be expressed as an integer over an integer. Then clearly 1/x cannot be expressed as an integer over an integer.

Evaluation _____

Proof 3: Assume that x is rational. Then $x = \frac{p}{q}$, where p and q are integers and $q \neq 0$. But then $\frac{1}{x} = \frac{1}{\frac{p}{q}} = \frac{q}{p}$, so it is rational. Since we proved the contrapositive, the statement is true.

Evaluation _____

Proof 4: We will prove the contrapositive. Assume that $1/x$ is rational. Since it is rational, $1/x = a/b$ for some integers a and b, with $b \neq 0$. Solving for x we get $x = b/a$, so x is rational.

Evaluation _____

Proof 5: I will prove the contrapositive statement: If $1/x$ is rational, then x is rational. Assume $1/x$ is rational. Then $\frac{1}{x} = \frac{a}{b}$ for some integers a and $b \neq 0$. We know that $1/x \neq 0$ (since otherwise $x \cdot 0 = 1$, which is impossible), so $a \neq 0$. Multiplying both sides of the previous equation by x we get $x\frac{a}{b} = 1$. Now if we multiply both sides by $\frac{b}{a}$ (which we can do since $a \neq 0$), we get $x = \frac{b}{a}$. Since a and b are integers with $a \neq 0$, x is rational.

Evaluation _____

★**Evaluate 2.98.** Mersenne primes are primes that are of the form $2^p - 1$, where p is prime. Are all numbers of this form prime? Give a proof/counterexample.

Proof 1: Restate the problem as if $2^p - 1$ is prime then p is prime. Assume p is not prime so $p = st$, where s and t are integers. Thus $2^p - 1 = 2^{st} - 1 = (2^s - 1)(2^{st-s} + 2^{st-2s} + \cdots + 2^s + 1)$. Because neither of these factors is 1 or $2^p - 1$
$\rightarrow 2^p - 1$ is not prime (contradiction)
$\rightarrow$ p is prime
$\rightarrow$ All numbers of the form $2^p - 1$ (with p a prime) are prime.

Evaluation _____

Proof 2: Numbers of the form 2^p only have 2 as a factor. Since $2^p - 1$ is clearly odd, it does not have 2 as a factor. Therefore it must not have any factors. So it is prime.

Evaluation _____

★**Exercise 2.99.** Let p be prime. Prove that not all numbers of the form $2^p - 1$ are prime.
Proof:

2.9 Reading Comprehension Questions

From Section 2.1

★**Question 2.1.** Because it was (perhaps incorrectly) assumed that you have heard the term *proof* before, it was never formally defined in the chapter. Let's make sure you don't go any further without having a good definition. So, what is a *proof*? Feel free to look up the definition (online or in a dictionary) if you need to.

★**Question 2.2.** Let's say someone correctly proves statement A. Does that mean A is a true statement, that you are just pretty sure that it is true, or that it may or may not be true based on whether or not you understand the argument being made in the proof? Explain your answer.

★**Question 2.3.** True or false: Every even number is not odd. Explain your answer.

★**Question 2.4.** If b is divisible by a, is it always the case that a is divisible by b? Explain using an example.

★**Question 2.5.** Can a number be both *composite* and *prime*? Explain.

★**Question 2.6.** Which are *prime*? Which of the following numbers are *composite*? Which are neither? Which are both?
1, 3, 4, 6, 38, 27, 97, 150, 173, 999983, 999985

★**Question 2.7.** Compute 6! and 7!. Did you compute 7! the easy way or the hard way?

★**Question 2.8.** For what values of n is $n!$ prime?

From Section 2.2

★**Question 2.9.** If the proposition A *implies* B is true, does that mean the proposition B *implies* A is true? Prove or give a counterexample.

★**Question 2.10.** True or false: If the inverse of an implication is true, then the implication is also true. Explain your answer.

★**Question 2.11.** True or false: If the inverse of an implication is true, then the converse of the implication is also true. Explain your answer.

★**Question 2.12.** What can you say about an implication and its contrapositive?

From Sections 2.3

★**Question 2.13.** In your own words, explain the idea behind contradiction proofs. Include specifics like how one goes about writing a proof by contradiction and why it is a valid proof technique. (The goal of this question is to help you better understand the technique and to convince you that it is indeed a valid technique, so put some thought into this one!)

★**Question 2.14.** Give all of the permutations of the set $\{\text{cow}, \text{chicken}, \text{rabbit}\}$

★**Question 2.15.** True or false: Every integer is a rational number. Explain your answer.

★**Question 2.16.** Prove that there is no smallest positive rational number. (Hint: Use contradiction!)

From Section 2.4

★**Question 2.17.** Explain why proof by contraposition is a valid proof technique.

★**Question 2.18.** Explain the difference between a proof by contradiction and a proof by contraposition, particularly as it applies to proving statements of the form $p \to q$.

★**Question 2.19.** True or false: Every irrational number is not an integer. Explain your answer.

★**Question 2.20.** Prove that if $x > 0$ is irrational, then $\sqrt{x}$ is irrational using

(a) proof by contradiction.

(b) proof by contraposition.

From Section 2.5

★**Question 2.21.** True or false: Every rational number is an integer. Prove your answer.

★**Question 2.22.** Prove that an integer n and n^2 have the same parity (that is, they are both even or both odd).

From Section 2.6

★**Question 2.23.** If you want to prove that A *if and only if* B is true (where A and B are statements of some sort), can you just show that A implies B? If not, explain why that does not work and what you would have to do instead (or in addition).

★**Question 2.24.** You want to prove that p if and only if q is true.

(a) Is showing that p implies q and $\neg q$ implies $\neg p$ a valid technique? Explain why or why not.

(b) Is showing that $\neg q \to \neg p$ and $q \to p$ a valid technique? Explain why or why not.

★**Question 2.25.** Prove that an integer n is even if and only if n^2 is even.

From Sections 2.7

★**Question 2.26.** Proof by counterexample is a valid proof technique. Proof by example is not. Explain the difference.

★**Question 2.27.** If I want to prove some equation, should I write down the equation and work both sides until they are the same? Explain why this is or is not a valid proof technique.

★**Question 2.28.** What is wrong with the following proof?

> Proof: Assume $a = b$, where a and b are not zero. Multiplying both sides by a, we get $a^2 = ab$. Subtracting b^2 from both sides, we get $a^2 - b^2 = ab - b^2$, which is equivalent to $(a - b)(a + b) = (a - b)b$. Dividing by $a - b$, we get $(a + b) = b$, which implies $2b = a$, but since $a = b$, $2b = b$, and dividing by b, we finally conclude that $2 = 1$. □

2.10 Problems

Problem 2.1. Prove that a number and its square have the same parity. That is, the square of an even number is even and the square of an odd number is odd.

Problem 2.2. Prove that the inverse of an implication is true if and only if the converse of the implication is true.

Problem 2.3. Let a and b be integers. Consider the problem of proving that if at least one of a or b is even, then ab is even. Is this equivalent to the statement from Evaluate 2.50? Explain, using the appropriate terminology from this chapter.

Problem 2.4. Let a and b be integers. Consider the statement "*If ab is even, then at least one of a or b is even.*" Rephrase this statement using the word *odd* instead of even (but you cannot use the phrase *not odd*). Using terminology from this chapter, how did you come up with the alternative phrasing?

Problem 2.5. Prove or disprove that there are 100 consecutive positive integers that are not perfect squares. (Recall: a number is a perfect square if it can be written as a^2 for some integer a.)

Problem 2.6. Consider the equation $n^4 + m^4 = 625$.

(a) Are there any *integers* n and m that satisfy this equation? Prove it.

(b) Are there any *positive integers* n and m that satisfy this equation? Prove it.

Problem 2.7. Consider the equation $a^3 + b^3 = c^3$ over the integers (that is, a, b, and c have to all be integers).

(a) Prove that the equations has infinitely many solutions.

(b) If we restrict a, b, and c to the positive integers, are there infinitely many solutions? Are there any? Justify your answer. (Hint: Do a web search for "Fermat's Last Theorem.")

Problem 2.8. Let n be an integer.

(a) Prove that if n is odd, then $3n + 4$ is odd.

(b) Is it possible to prove that n is odd iff $3n + 4$ is odd? If so, prove it. If not, explain why not (i.e. give a counter example).

(c) If we don't assume n has to be an integer, is it possible to prove that n is odd iff $3n + 4$ is odd? If so, prove it. If not, explain why not (i.e. give a counter example).

Problem 2.9. Prove that if n is an integer and $5n + 4$ is even, then n is even using a

(a) direct proof

(b) proof by contraposition

(c) proof by contradiction

Problem 2.10. Prove that a is even if and only if a^2 is even.

Problem 2.11. Prove that $n^2 + 2n + 1$ is even if and only if n is odd.

Problem 2.12. Let n be an integer.

(a) Prove that if n is odd, then $4n + 3$ is odd.

(b) Is it possible to prove that n is odd iff $4n + 3$ is odd? If so, prove it. If not, explain why not (i.e. give a counter example).

Problem 2.13. Prove that ab is odd iff a and b are both odd.

Problem 2.14. Prove or disprove each of the following.

(a) Let k be an odd integer. Then a is even if and only if ka is even.

(b) Let k be an even integer. Then a is even if and only if ka is even.

(c) Let k be an integer. Then a is even if and only if ka is even.

Problem 2.15. Let n be an odd integer. For what values of k do n and nk have the same parity? Prove your claim.

Problem 2.16. Let n be an even integer. For what values of k do n and nk have the same parity? Prove your claim.

Problem 2.17. Prove or disprove: Every positive integer can be written as the sum of the squares of two integers.

Problem 2.18. Prove that the product of two rational numbers is rational.

Problem 2.19. Prove that the product of a non-zero rational number and an irrational number is irrational.

Problem 2.20. Prove or disprove that c is irrational if and only if $c + 1$ is irrational.

Problem 2.21. Prove or disprove that c is rational if and only if c^2 is rational.

Problem 2.22. Prove or disprove that $n^2 - 1$ is composite whenever n is a positive integer greater than or equal to 1.

Problem 2.23. Prove or disprove that $n^2 - 1$ is composite whenever n is a positive integer greater than or equal to 3.

Problem 2.24. Compute 7!.

Problem 2.25. Compute 8!/6!.

Problem 2.26. List the permutations of the set $\{a, b, c, d\}$.

Problem 2.27. Prove or disprove that $P = NP$.[2]

[2] A successful solution to this will earn you an A in the course. You are free to use Google or whatever other resources you want for this problem, but you must fully understand the solution you submit.

Chapter 3: Sets, Functions, and Relations

3.1 Sets

3.1.1 Definitions

Definition 3.1. *Sets*

- *A* **set** *is an unordered collection of objects.*
- *The objects in the set are called the* **elements** *of the set.*
- *If a belongs to the set A, then we write $a \in A$, read "a is an element of A."*
- *If a does not belong to the set A, we write $a \notin A$, read "a is not an element of A."*
- *Generally speaking, repeated elements in a set are ignored.*

Note: *The symbol $\in$ should be read as* **is an element of**, *not* exists in.

Example 3.2. The sets $A = \{1, 2, 3\}$, $B = \{3, 2, 1\}$, and $C = \{1, 1, 1, 2, 2, 3\}$ actually represent the same set since repeated values are ignored and the order elements are listed does not matter. Notice that $1 \in A$ and $3 \in A$, but $4 \notin A$.

Let $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the set of decimal digits. Then $4 \in D$ but $11 \notin D$.

Notice that the elements in a set are listed between curly braces. Thus, $\{1, 2, 3\}$ is a set (where order does not matter and duplicates are ignored), but $[1, 2, 3]$ is a list (where order *does* matter and duplicates are allowed). Also, 1, 2, 3 is just a list of three numbers whereas $\{1, 2, 3\}$ is the set containing the numbers 1, 2, and 3.

Definition 3.3. *Cardinality*

- *The number of elements in a set A, also known as the the* **cardinality** *of A, will be denoted by $|A|$.*
- *If $|A|$ is finite, we call A a* **finite set**.
- *If the set A has infinitely many elements, we write $|A| = \infty$ and we refer to A as an* **infinite set**.

Example 3.4. If A, B, C, and D are the sets from Example 3.2, then $|A| = 3$, $|B| = 3$, $|C| = 3$, and $|D| = 10$.

★**Exercise 3.5.** Give the set of prime numbers less than 10. What is its cardinality?

Answer _____

Since we cannot list every element of an infinite set, we need a way of expressing the set so that it is clear what elements it contains. If the elements of the set follow some pattern, it is common to list the first several elements and then conclude with ..., indicating that the pattern continues. There is no "right" number of elements to list when using this notation, but there needs to be enough so that the pattern is evident. Often 3-5 elements suffices.

Example 3.6. The set of positive integers can be expressed as $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Notice that $|\mathbb{Z}^+| = \infty$.

The set of positive integers that are a multiple of 5 can be expressed as $\{5, 10, 15, 20, \ldots\}$. Hopefully it is clear that $|\{5, 10, 15, 20, \ldots\}| = \infty$.

The set of integer multiples of 5 can be expressed as $\{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$. Hopefully it is clear that this is also an infinite set.

Definition 3.7. *We say two sets are* **equal** *if they contain the same elements. That is* $\forall x(x \in A \leftrightarrow x \in B)$. *If* A *and* B *are equal sets, we write* $A = B$.

Note: *We will normally denote sets by capital letters, like* $A, B, S, \mathbb{N}$, *etc. Elements will be denoted by lowercase letters, like* a, b, r, *etc.*

★**Exercise 3.8.** Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{1, 2, 3, 4, 5, 4, 3, 2, 1\}$, $C = \{6, 3, 4, 5, 1, 3, 2\}$.

Then $|A| =$ _____, $|B| =$ _____, and $|C| =$ _____.

Which of A, B, and C represent the same sets? _____

Definition 3.9. *The following notation is pretty standard, and we will follow it in this book.*

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$	*the* **natural numbers**.
$\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$	*the* **integers**.
$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$	*the* **positive integers**.
$\mathbb{Z}^- = \{-1, -2, -3, \ldots\}$	*the* **negative integers**.
$\mathbb{Q}$	*the* **rational numbers**.
$\mathbb{R}$	*the* **real numbers**.
$\mathbb{C}$	*the* **complex numbers**.
$\varnothing = \{\}$	*the* **empty set** *or* **null set**.

Note: *There is no universal agreement of the definition of* $\mathbb{N}$*. Although here it is defined as* $\{0, 1, 2, 3, \ldots\}$*, it is sometimes defined as* $\mathbb{N} = \mathbb{Z}^+$*. The only difference is whether or not* 0 *is included. I prefer the definition given here because then we have a notation for the positive integers* ($\mathbb{Z}^+$) *as well as the non-negative integers* ($\mathbb{N}$)*.*

Example 3.10. Notice that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{R}| = \infty$. But this may be a bit misleading. Do all of these sets have the same number of elements? Believe it or not, it turns out that $\mathbb{N}$ and $\mathbb{Z}$ do, but that $\mathbb{R}$ has many more elements than both of these. If it seems strange to talk about whether or not two infinite sets have the same number of elements, don't worry too much about it. We probably won't bring it up again.

★**Exercise 3.11.** (a) $|\mathbb{C}| =$ _____, (b) $|\mathbb{Z}^+| =$ _____, (c) $|\varnothing| =$ _____

Another other common notation that is used express sets is called *set builder notation*. It is easier to understand through examples than by giving a formal definition.

Example 3.12. Let S be the set of the squares of integers. We can express this as $S = \{n^2 | n \in \mathbb{Z}\}$ or $S = \{n^2 : n \in \mathbb{Z}\}$. We call this *set builder notation*. We read the : or | as "such that." Thus, S is the set containing numbers of the form n^2 such that n is an integer.

Example 3.13. Consider the set of integers that are one less than a positive power of 2. This set contains elements such as $1 = 2^1 - 1$, $3 = 2^2 - 1$, and $255 = 2^8 - 1$. We can express this set in set builder notation as $\{2^n - 1 | n \in \mathbb{Z}^+\}$.

We could also use the notation $\{2^1 - 1, 2^2 - 1, 2^3 - 1, \ldots\}$, since the pattern is evident. However, it would be unwise to write it as $\{1, 3, 7, 15, \ldots\}$ since it may or may not be evident what the pattern is when expressed in this way.

★**Exercise 3.14.** Use two different notations to express the set of even integers.

Answer _____

Example 3.15. Let T be the set of all integers that can be expressed as the sum of the square of two positive integers. This set contains elements such as $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, and $25 = 3^2 + 4^2$. Then $T = \{n^2 + m^2 | n, m \in \mathbb{Z}^+\}$.

In this case, expressing the set as something like $\{2, 5, 8, 9, \ldots\}$ does not make sense at all because there is no way of discerning a pattern.

Example 3.16. Use set builder notation to express $\mathbb{C}$, the set of complex numbers.

Solution: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$.

★**Exercise 3.17.** Use set builder notation to express $\mathbb{Q}$, the set of all rational numbers.

Answer _____

Definition 3.18. *Subsets*

- *If every element in A is also in B, we say that A is a* **subset** *of B and we write this as $A \subseteq B$.*
- *If $A \subseteq B$ and there is some $x \in B$ such that $x \notin A$, then we say A is a* **proper subset** *of B, denoting it by $A \subset B$.*
- *If there is some $x \in A$ such that $x \notin B$, then A is not a subset of B, which we write as $A \not\subseteq B$.*

Note: *Some authors use $\subset$ to mean the same thing as $\subseteq$. You will need to consider the context in order to interpret it correctly.*

Example 3.19. Let $S = \{1, 2, \ldots, 20\}$, that is, the set of integers between 1 and 20, inclusive. Let $E = \{2, 4, 6, \ldots, 20\}$, the set of all even integers between 2 and 20, inclusive. Notice that $E \subseteq S$. Let $P = \{2, 3, 5, 7, 11, 13, 17, 19\}$, the set of primes less than 20. Then $P \subseteq S$, but $P \not\subseteq E$ and $E \not\subseteq P$.

★**Exercise 3.20.** Let $S = \{n^2 | n \in \mathbb{Z}\}$ and $A = \{1, 4, 9, 16\}$. Answer each of the following, including a brief justification.

(a) Is $A \subseteq S$? _____

(b) Is $A \subset S$? _____

(c) Is $S \subseteq S$? _____

(d) Is $S \subset S$? _____

(e) Is $S \subset A$? _____

★**Exercise 3.21.** Let A be the set of integers divisible by 6, B be the set of integers divisible by 2, and C be the set of integers divisible by 3. Answer each of the following, giving a brief justification.

(a) Is $A \subseteq B$?_____

(b) Is $A \subseteq C$?_____

(c) Is $B \subseteq A$?_____

(d) Is $B \subseteq C$?_____

(e) Is $C \subseteq A$?_____

(f) Is $C \subseteq B$?_____

Example 3.22. The set

$$S = \{\text{Roxan}, \text{Jacquelin}, \text{Sean}, \text{Fatimah}, \text{Wakeelah}, \text{Ashley}, \text{Ruben}, \text{Leslie}, \text{Madeline}\}$$

is the set of students in a particular course. This set can be split into two subsets: the set $F = \{\text{Roxan}, \text{Jacquelin}, \text{Fatimah}, \text{Wakeelah}, \text{Ashley}, \text{Madeline}\}$ of females in the class, and the set $M = \{\text{Sean}, \text{Ruben}, \text{Leslie}\}$ of males in the class. Thus we have $F \subseteq S$ and $M \subseteq S$. Notice that it is *not true* that $F \subseteq M$ or that $M \subseteq F$. Put another way, $F \nsubseteq M$ and $M \nsubseteq F$

Example 3.23. Find all the subsets of $\{a, b, c\}$.

Solution: They are $\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}$, and $\{a, b, c\}$.

Notice that there are 8 subsets. Also notice that $8 = 2^3$. As we will see shortly, that is not a coincidence.

Notice that we wrote $\varnothing$ and not $\{\varnothing\}$ in the previous example. It turns out that $\varnothing \neq \{\varnothing\}$. $\varnothing$ is the empty set–that is, the set that has no elements. $\{\varnothing\}$ is the set containing the empty set. Thus, $\{\varnothing\}$ is a set containing the single element $\varnothing$. You can use either $\varnothing$ or $\{\}$ to denote the empty set, but not $\{\varnothing\}$.

★**Exercise 3.24.** Find all the subsets of $\{a, b, c, d\}$.

Definition 3.25. *The* power set *of a set is the set of all subsets of a set. The power set of a set A is denoted by $P(A)$.*

Example 3.26. If $A = \{a, b, c\}$, example 3.23 implies that $P(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. Notice that the solution is a set, the elements of which are also sets.

An *incorrect answer* would be $\{\varnothing, a, b, c, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. This is incorrect because a is not the same thing as $\{a\}$ (the set containing a). $\{a\} \in P(A)$, but $a \notin P(A)$. This is a subtle but important distinction.

★**Exercise 3.27.** Find $P(\{a, b, c, d\})$.

We will prove the following theorem in the next section after we have developed the appropriate notation to do so.

Theorem 3.28. *Let A be a set with n elements. Then $|P(A)| = 2^n$.*

★**Exercise 3.29.** Let A be a set with 4 elements.

(a) $|P(A)| =$ _____.

(b) $|P(P(A))| =$ _____.

(c) $|P(P(P(A)))| =$ _____.

★**Exercise 3.30.** If one element is added to a finite set A, how much larger is the power set of A after the element is added (relative to the size of the power set before it is added)? Explain your answer.

Answer _____

_____

_____

3.1.2 Set Operations

We can obtain new sets by performing operations on other sets. In this section we discuss the common set operations. *Venn diagrams* are often used as a pictorial representation of the relationships between sets. We provide Venn diagrams to help visualize the set operations. In our Venn diagrams, the region(s) in the darker color represent the elements of the set of interest.

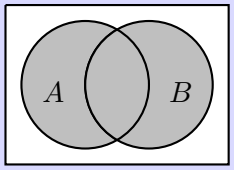
Definition 3.31.

The **union** *of two sets A and B is the set containing elements from either A or B. More formally,*

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

Notice that in this case the **or** *is an* **inclusive or**. *That is, x can be in A, or it can be in B, or it can be in both.*

$A \cup B$



Example 3.32. Let $A = \{1, 2, 3, 4, 5, 6\}$, and $B = \{1, 3, 5, 7\}$. Then $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$.

★**Exercise 3.33.** Let A be the set of even integers and B be the set of odd integers. Then

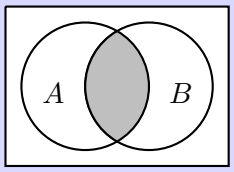
$A \cup B =$ _____

Definition 3.34.

The **intersection** *of two sets A and B is the set containing elements that are in both A and B. More formally,*

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

$A \cap B$



Example 3.35. Let $A = \{1, 2, 3, 4, 5, 6\}$, and $B = \{1, 3, 5, 7, 9\}$. Then $A \cap B = \{1, 3, 5\}$.

★**Exercise 3.36.** Let A be the set of even integers and B be the set of odd integers. Then

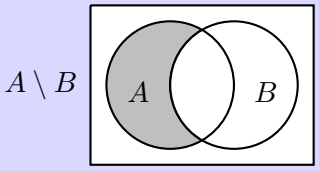
$A \cap B =$ _____

Definition 3.37.

The **difference** *(or* **set-difference***) of sets A and B is the set containing elements from A that are not in B. More formally,*

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

The set difference of A and B is sometimes denoted by $A - B$.



Example 3.38. Let $A = \{1, 2, 3, 4, 5, 6\}$, and $B = \{1, 3, 5, 7, 9\}$. Then $A \setminus B = \{2, 4, 6\}$ and $B \setminus A = \{7, 9\}$.

★**Exercise 3.39.** Let A be the set of even integers and B be the set of odd integers. Then

$A \setminus B =$ _____ and $B \setminus A =$ _____.

We can now prove Theorem 3.28.

Example 3.40. Let A be a set with n elements. Then $|P(A)| = 2^n$.

Proof: We use induction[a] and the idea from the solution to Exercise 3.24. Clearly if $|A| = 1$, A has $2^1 = 2$ subsets: $\varnothing$ and A itself.

Assume every set with $n - 1$ elements has 2^{n-1} subsets. Let A be a set with n elements. Choose some $x \in A$. Every subset of A either contains x or it doesn't. Those that do not contain x are subsets of $A \setminus \{x\}$. Since $A \setminus \{x\}$ has $n-1$ elements, the induction hypothesis implies that it has 2^{n-1} subsets. Every subset that does contain x corresponds to one of the subsets of $A \setminus \{x\}$ with the element x added. That is, for each subset $S \subseteq A \setminus \{x\}$, $S \cup \{x\}$ is a subset of A containing x. Clearly there are 2^{n-1} such new subsets. Since this accounts for all subsets of A, A has $2^{n-1} + 2^{n-1} = 2^n$ subsets. □

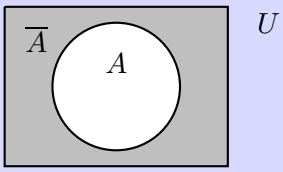
[a] We will cover induction more fully and formally later. But since this use of induction is pretty intuitive, especially in light of Example 3.24, it serves as a useful foreshadowing of things to come.

Definition 3.41.

Let $A \subseteq U$. The **complement** *of A with respect to U is just the set difference $U \setminus A$. More formally,*

$$\overline{A} = \{x \in U : x \notin A\} = U \setminus A.$$

In words, $\overline{A}$ is the set of everything not in A. Other common notations for set complement include A^c and A'.



Note: *Often the set U, which is called the* **universe** *or* **universal set**, *is implied and we just use $\overline{A}$ to denote the complement. We usually follow this convention here. Further, when talking about several sets, we will usually assume they have the same universal set.*

Example 3.42. Let $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the universal set of decimal digits and $A = \{0, 2, 4, 6, 8\} \subset U$ be the set of even digits. Then $\overline{A} = \{1, 3, 5, 7, 9\}$ is the set of odd digits.

★**Exercise 3.43.** Let A be the set of even integers and B be the set of odd integers, and let the universal set be $U = \mathbb{Z}$. Then $\overline{A}$= _____ and $\overline{B}$= _____.

It should not be too difficult to convince yourself that the following theorem is true.

Theorem 3.44. *Let A be a subset of some universal set U. Then*

$$\begin{aligned} \overline{A} \cap A &= \varnothing, \text{ and} \\ \overline{A} \cup A &= U. \end{aligned}$$

The various intersecting regions for two and three sets can be seen in Figures 3.1 and 3.2.

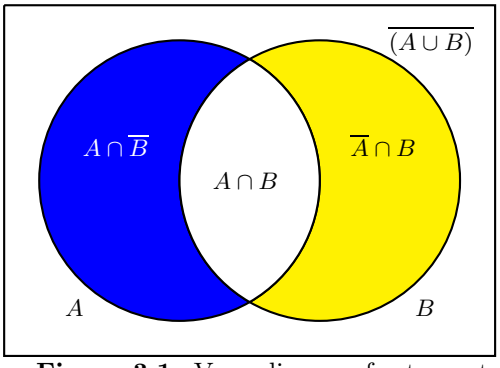


Figure 3.1: Venn diagram for two sets.

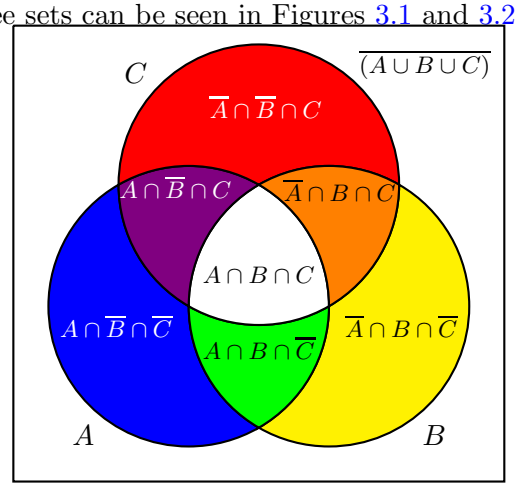


Figure 3.2: Venn diagram for three sets.

Definition 3.45. *Two sets A and B are* **disjoint** *or* **mutually exclusive** *if $A \cap B = \varnothing$. That is, they have no elements in common.*

Example 3.46. Let A be the set of prime numbers, B be the set of perfect squares, and C be the set of even numbers. Then A and B are clearly disjoint since if a number is a perfect square, it cannot possibly be prime (although 0 and 1 are not prime for different reasons than the rest of the elements of B). On the other hand, A and C are not disjoint since they both contain 2, and B and C are not disjoint because they both contain 4.

★**Exercise 3.47.** Let A be the set of even integers and B be the set of odd integers. Are A and B disjoint? Explain.

Answer _____

_____

Set identities can be used to show that two sets are the same. Table 3.1 gives some of the most common set identities. In these identities, U is the universal set. We won't provide proofs for most of these, but we will present a few examples and a technique that will allow you to verify that they are correct in Section 3.1.3.

Name	*Identity*
commutativity	$A \cup B = B \cup A$ $A \cap B = B \cap A$
associativity	$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$
distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
identity	$A \cup \varnothing = A$ $A \cap U = A$
complement	$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$
domination	$A \cup U = U$ $A \cap \varnothing = \varnothing$
idempotent	$A \cup A = A$ $A \cap A = A$
complementation	$\overline{(\overline{A})} = A$
DeMorgan's	$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$
absorption	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$

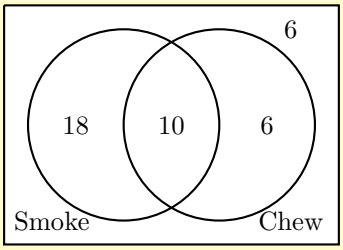
Table 3.1: Set Identities

These identities may look somewhat familiar. They are essentially the same as the logical equivalences presented in Table 1.3. In fact, if we equate T to U, F to $\varnothing$, $\vee$ to $\cup$, $\wedge$ to $\cap$, and $\neg$ to $^-$(complement), the laws are identical. This is because logic operations and sets are both what we call *Boolean algebras*. We won't go into detail about this connection, but in case you run into the concept in the future, you heard it here first!

Sometimes you need to find the number of elements in the union of several sets. This is easy if the sets do not intersect. If they do intersect, more care is needed to make sure no elements are missed or counted more than once. In the following examples we will use Venn diagrams to help us do this correctly. Later, we will learn about a more powerful tool to do this—*inclusion-exclusion*.

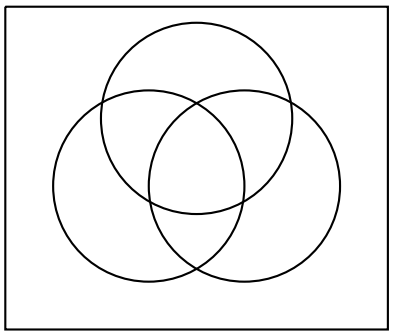
Example 3.48. Of 40 people, 28 smoke and 16 chew tobacco. It is also known that 10 both smoke and chew. How many among the 40 neither smoke nor chew?

Solution: We fill up the Venn diagram below as follows. Since $|Smoke \cap Chew| = 10$, we put a 10 in the intersection. Then we put $28 - 10 = 18$ in the part that *Smoke* does not overlap *Chew* and $16 - 10 = 6$ in the part of *Chew* that does not overlap *Smoke*. We have accounted for $10 + 18 + 6 = 34$ people that are in at least one of the sets. The remaining $40 - 34 = 6$ people outside these sets don't smoke or chew (and probably don't date girls who do).



We truly hope that these numbers are not representative of the number of people who smoke and/or chew in real life. It's bad for you. Don't do it. Really.

★**Exercise 3.49.** In a group of 30 people, 8 speak English, 12 speak Spanish and 10 speak French. It is known that 5 speak English and Spanish, 7 Spanish and French, and 5 English and French. The number of people speaking all three languages is 3. How many people speak at least one of these languages?



Definition 3.50. *The* **Cartesian product** *of sets A and B is the set $A \times B = \{(a, b) | a \in A \wedge b \in B\}$. In other words, it is the set of all ordered pairs of elements from A and B.*

Example 3.51. If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then
$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$, and
$B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.
Notice that $A \times B \neq B \times A$. If $A \neq B$, this is always the case.

★**Exercise 3.52.** Let $A = \{1, 2, 3, 4\}$, and $B = \{3\}$. Compute $A \times B$.

$A \times B =$ _____

Definition 3.53. *If A is a set, then $A^2 = A \times A$, and $A^n = A \times A^{n-1}$.*

Example 3.54. If $B = \{a, b\}$ then

$$B^2 = \{(a, a), (a, b), (b, a), (b, b)\}, \text{ and}$$

$$B^3 = \{(a, a, a), (a, b, a), (b, a, a), (b, b, a), (a, a, b), (a, b, b), (b, a, b), (b, b, b)\}$$

★**Exercise 3.55.** Let $A = \{0, 1\}$. Find A^2 and A^3.

$A^2 =$

$A^3 =$

It shouldn't be too difficult to convince yourself of the following.

Theorem 3.56. *If A and B are finite sets with $|A| = n$ and $|B| = m$, then $|A \times B| = n \cdot m$.*

Example 3.57. Let A and B be finite sets with $|A| = 100$ and $|B| = 5$. Then $|A \times B| = 100 * 5 = 500$, $|A^2| = 100 * 100 = 10,000$, and $|B^4| = 5^4 = 625$.

★**Exercise 3.58.** Let A, B, and C be sets with $|A| = 10$, $|B| = 50$, and $|C| = 20$. Determine the following

(a) $|A \times B| =$ _____

(b) $|A \times C| =$ _____

(c) $|B^3| =$ _____

(d) $|A \times B \times C| =$ _____

★**Evaluate 3.59.** If $A \times B = \varnothing$, what can we conclude about A and B?

Solution 1: Assume A and B are not empty. We know the Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Therefore, we can conclude that our assumption was incorrect because if each set is not empty, (a, b) is in the cross product, but $A \times B = \varnothing$, so at least one of the sets must be empty.

Evaluation _____

_____

Solution 2: Notice that if $A = \varnothing$ and $B = \varnothing$, $A \times B = \varnothing$. Therefore, if $A \times B = \varnothing$, then $A = \varnothing$ and $B = \varnothing$.

Evaluation _____

_____

Solution 3: We can conclude that both A and B are empty. I'll prove it by contradiction. Assume that $A \times B = \varnothing$, but that it is not the case that both A and B are empty. Then neither A nor B is empty. But then there is some $a \in A$ and some $b \in B$, and $(a, b) \in A \times B$, which implies that $A \times B \neq \varnothing$. This contradicts our assumption. Therefore both A and B are empty.

Evaluation _____

_____

Solution 4: At least one of A or B is empty by contradiction. Assume that $A \times B = \varnothing$, but that it is not the case that at least one of A or B is empty. Then neither A nor B is empty. Then there is some $a \in A$ and some $b \in B$. But then $(a, b) \in A \times B$, which implies that $A \times B \neq \varnothing$. This contradicts our assumption. Therefore at least one of A or B is empty.

Evaluation _____

_____

3.1.3 Set Proofs

The following theorem can be used to prove set identities.

Theorem 3.60. *Two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.*

Let's see this theorem in action.

Example 3.61. Prove that $A \setminus B = A \cap \overline{B}$.

Proof: Let $x \in A \setminus B$. Then by definition of difference, $x \in A$ and $x \notin B$. But if $x \notin B$, then $x \in \overline{B}$ by definition of complement. Since $x \in A$ and $x \in \overline{B}$, $x \in A \cap \overline{B}$ by definition of intersection. Since whenever $x \in A \setminus B$, $x \in A \cap \overline{B}$, we have shown that $A \setminus B \subseteq A \cap \overline{B}$.

Now assume that $x \in A \cap \overline{B}$. Then $x \in A$ and $x \in \overline{B}$ by definition of intersection. By definition of complement, $x \notin B$. But if $x \in A$ and $x \notin B$, then $x \in A \setminus B$ by definition of difference. Since whenever $x \in A \cap \overline{B}$, $x \in A \setminus B$, we have that $A \cap \overline{B} \subseteq A \setminus B$.

Since we have shown that $A \setminus B \subseteq A \cap \overline{B}$ and that $A \cap \overline{B} \subseteq A \setminus B$, by Theorem 3.60 $A \setminus B = A \cap \overline{B}$. □

That was the long, drawn-out version of the proof. The purpose of all of the detail is to make the technique clear. Here is a proof without any extraneous details.

Proof: We will prove this by showing set containment both ways.

Let $x \in A \setminus B$. Then $x \in A$ and $x \notin B$. This implies that $x \in \overline{B}$. Therefore $x \in A \cap \overline{B}$. Since $A \setminus B$ implies $x \in A \cap \overline{B}$, $A \setminus B \subseteq A \cap \overline{B}$.

Now assume that $x \in A \cap \overline{B}$. Then $x \in A$ and $x \in \overline{B}$. Then $x \notin B$, and therefore $x \in A \setminus B$. Since $x \in A \cap \overline{B}$ implies $x \in A \setminus B$, $A \cap \overline{B} \subseteq A \setminus B$. □

The proofs in the previous example are called *set containment proofs* since we showed set containment both ways. The technique is pretty straightforward: Theorem 3.60 tells us that if $X \subseteq Y$ and $Y \subseteq X$, then $X = Y$. Thus, to prove $X = Y$, we just need to show that $X \subseteq Y$ and $Y \subseteq X$. But how do we show that one set is a subset of another? This is easy: To show that $X \subseteq Y$, we show that every element from X is also in Y. In other words, we assume that $x \in X$ and use definitions and logic to show that $x \in Y$. Assuming we do not use any special properties about x other than the fact that $x \in X$, then x is an arbitrary element from X, so this shows that $X \subseteq Y$. Showing that $Y \subseteq X$ uses exactly the same technique.

Note: *Be careful. To prove that $X = Y$, you generally need to prove two things: $X \subseteq Y$ and $Y \subseteq X$. Do not forget to do both. On the other hand, if you are asked to prove that $X \subseteq Y$, you do not need to (and should not) show that $Y \subseteq X$.*

Let's see another example of this type of proof. This proof will provide a few more details than necessary in order to further explain the technique.

Example 3.62. Prove the first De Morgan's Laws: Given sets A and B, $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.

Proof: Let $x \in \overline{(A \cup B)}$. Then $x \notin A \cup B$ (by definition of complement). Thus

$x \notin A$ and $x \notin B$ (by definition of union), which is the same thing as $x \in \overline{A}$ and $x \in \overline{B}$ (by definition of complement). But then we have that $x \in \overline{A} \cap \overline{B}$ (by definition of intersection). Notice that x was an arbitrary element from $\overline{(A \cup B)}$, and we showed that $x \in \overline{A} \cap \overline{B}$. Therefore, every element in $\overline{(A \cup B)}$ is also in $\overline{A} \cap \overline{B}$. In other words, $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$.

Now, let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A}$ and $x \in \overline{B}$. This means that $x \notin A$ and $x \notin B$ which is the same as $x \notin A \cup B$. But this last statement asserts that $x \in \overline{(A \cup B)}$. Hence $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$.

Since we have shown that the two sets contain each other, they are equal by Theorem 3.60. □

You have already seen a few correct ways to prove that $A \setminus B = A \cap \overline{B}$. Can you spot the problem(s) in the following 'proofs' of this? These proofs use the alternative notation of $A - B$ for set difference.

★**Evaluate 3.63.** Use a set containment proof to prove that if A and B are sets, then $A - B = A \cap \overline{B}$.

Proof 1: Assume $x \in \{A - B\}$ so $x \in A$ and x is not $\in B$. This means $x \in A$ and $\overline{B}$. Therefore $x \in A \cap \overline{B}$. Thus $A - B = A \cap \overline{B}$.

Evaluation _____

Proof 2: $\overline{B}$ is the other part of the universal that does not contain any part of B. $A \cup \overline{B}$ means all intersection part of A and the universal that does not contain any part of B. Therefore it returns all elements that are in A but not in B which are $A - B$. Thus, $A - B = A \cap \overline{B}$.

Evaluation _____

Proof 3: To prove that $A - B = A \cap \overline{B}$, first let $x \in A - B$. By definition of the difference of sets, this means that x is an element of A that is not in B, or in other words, $x \in A$ and $x \notin B$. This is the same as $x \in A \cap \overline{B}$, thus proving that $A - B \subseteq A \cap \overline{B}$.

Now let $x \in A \cap \overline{B}$. This means that $x \in A$ and $x \notin B$, so it is in A, but not in B, which is what we just proved in the previous statement, thus proving that $A - B = A \cap \overline{B}$.

Evaluation _____

Sometimes we can do a set containment proof in one step instead of two. This only works if every step of the proof is reversible. We illustrate this idea next.

Example 3.64. Prove that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Proof: We have

$$\begin{aligned} x \in A \setminus (B \cup C) &\leftrightarrow x \in A \wedge x \notin (B \cup C) \\ &\leftrightarrow (x \in A) \ \wedge \ ((x \notin B) \ \wedge \ (x \notin C)) \\ &\leftrightarrow (x \in A \ \wedge \ x \notin B) \ \wedge \ (x \in A \ \wedge \ x \notin C) \\ &\leftrightarrow (x \in A \setminus B) \ \wedge \ (x \in A \setminus C) \\ &\leftrightarrow x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

□

Note: *The proof in the previous example works because every step is reversible. You can only write something like 'α ↔ β' in a proof if α → β and β → α are both true. When attempting to shortcut proofs with this technique, make sure each step truly is reversible.*

★**Fill in the details 3.65.** Use a set containment proof to show that

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Solution: We have,

$x \in (A \cup B) \cap C$

$\leftrightarrow$ $x \in (A \cup B) \wedge$ _____ by def. of intersection

$\leftrightarrow$ $(x \in A \vee$ _____ $) \wedge x \in C$ by _____

$\leftrightarrow$ $(x \in A \wedge x \in C) \vee$ _____ by _____

$\leftrightarrow$ _____ $\vee (x \in B \cap C)$ by _____

$\leftrightarrow$ $x \in (A \cap C) \cup (B \cap C)$. by _____

3.2 Modular Arithmetic, GCD, Rounding

In this section we introduce some notation that allows us to think about remainders when doing division in a different way than you may be used to. Then we will discuss the greatest common divisor of two integers, including a simple algorithm to compute it. Finally, we will see the floor and ceiling functions, which allow us to round down or up, depending on our need.

We begin by repeating a few definitions from Section 2.1 in case you skipped it.

Definition 3.66. *Recall that:*

- *An* **even integer** *is one of the form $2k$, where k is an integer.*
- *An* **odd integer** *is one of the form $2k+1$ where k is an integer.*
- *Two integers have the same* **parity** *if they are both even or both odd.*

Example 3.67. Since $14 = 2 \cdot 7$, it is even. Similarly, since $23 = 2 \cdot 11 + 1$, it is odd.

Example 3.68. Since 50 and 124 are both even, they have the same parity.

Definition 3.69. *Let b and a be integers with $a \neq 0$. We say that b is* **divisible by** *a if there exists an integer c such that $b = ac$. If b is divisible by a, we also say that b is a* **multiple** *of a, a is a* **factor** *or* **divisor** *of b, and that a* **divides** *b, written as $a|b$. If a does not divide b, we write $a \nmid b$.*

Example 3.70. Since $6 = 2 \cdot 3$, $2|6$, and $3|6$. But $4 \nmid 6$ since we cannot write $6 = 4 \cdot c$ for any integer c.

Example 3.71. 100 is divisible by 25. We can say the same thing by saying 25 divides 100, which we can also write as $25|100$. We can also say that 25 is a factor of 100.

Definition 3.72. *A positive integer $p > 1$ is* **prime** *if its only positive factors are 1 and p. A positive integer $c > 1$ which is not prime is said to be* **composite**.

Example 3.73. Since $21 = 3 \cdot 7$, it is composite and therefore not prime. On the other hand, 17 has no factors other than 1 and 17 so it is prime.

Note: *Notice that according to the definitions given above, 1 is neither prime nor composite. This is one of the many things that makes 1 special.*

Definition 3.74. *For a non-negative integer n, the quantity $n!$ (read "n* **factorial**" *) is defined as follows. $0! = 1$ and if $n > 0$ then $n!$ is the product of all the integers from 1 to n inclusive:*

$$n! = 1 \cdot 2 \cdots n.$$

Example 3.75. $3! = 1 \cdot 2 \cdot 3 = 6$, and $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

Definition 3.76. *The* **mod** *operator is defined as follows: for integers a and n such that $a \geq 0$ and $n > 0$, **a mod n** is the integral non-negative remainder when a is divided by n. Observe that this remainder is one of the n numbers*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-1.$$

When we are working with the mod operator, we say we are are doing **modular arithmetic**.

Example 3.77. Here are some example computations:

$234 \bmod 100 = 34$	$1961 \bmod 37 = 0$	$6 \bmod 5 = 1$
$38 \bmod 15 = 8$	$1966 \bmod 37 = 5$	$11 \bmod 5 = 1$
$15 \bmod 38 = 15$	$1 \bmod 5 = 1$	$16 \bmod 5 = 1$

★**Exercise 3.78.** Compute the following:

(a) $345 \bmod 100 =$ _____ (d) $15 \bmod 9 =$ _____ (g) $19 \bmod 12 =$ _____

(b) $23 \bmod 15 =$ _____ (e) $27 \bmod 9 =$ _____ (h) $31 \bmod 12 =$ _____

(c) $15 \bmod 4 =$ _____ (f) $7 \bmod 12 =$ _____ (i) $47 \bmod 12 =$ _____

Definition 3.79. *For integers a, b, and n, where $n > 0$, we say that a is* **congruent to** b **modulo** n *if n divides $a - b$ (that is, $a - b = kn$ for some integer k). We write this as $a \equiv b \pmod{n}$.*

There are a few other (equivalent) ways of defining congruence modulo n.

- *$a \equiv b \pmod{n}$ iff a and b have the same remainder when divided by n.*
- *$a \equiv b \pmod{n}$ iff $a - b$ is a multiple of n.*
- *$a \equiv b \pmod{n}$ iff $a - b = kn$ for some integer k.*

If $a - b \neq kn$ for any integer k, then a is not congruent to b modulo n, and we write this as $a \not\equiv b \pmod{n}$.

Example 3.80. Notice that $21 - 6 = 15 = 3 \cdot 5$, so $21 \equiv 6 \pmod 5$.

Notice that if $a \equiv b \pmod n$ and $0 \leq b < n$, then b is the remainder when a is divided by n.

★**Exercise 3.81.** Prove that for every integer n, $n^2 \pmod 4$ is either 0 or 1. (Hint: Consider the cases when n is even and odd.)

Example 3.82. Prove that the sum of two squares of integers leaves remainder 0, 1 or 2 when divided by 4.

Proof: According to Example 3.81, the squares of integers have remainder 0 or 1 when divided by 4. Thus, when we add two squares, the possible remainders when divided by 4 are 0 $(0+0)$, 1 $(0+1$ or $1+0)$, and 2 $(1+1)$. □

Example 3.83. Prove that 2003 is not the sum of two squares.

Proof: Notice that $2003 \equiv 3 \pmod 4$. Thus, by Example 3.82 we know that 2003 cannot be the sum of two squares. □

We now prove some simple properties of congruences.

Theorem 3.84. *Let $a, b, c, d \in \mathbb{Z}$, and $n, k \in \mathbb{Z}^+$ with $a \equiv b \mod n$ and $c \equiv d \mod n$. Then*

1. $a + c \equiv b + d \mod n$
2. $a - c \equiv b - d \mod n$
3. $ac \equiv bd \mod n$
4. $a^k \equiv b^k \mod n$
5. *If f is a polynomial with integral coefficients then $f(a) \equiv f(b) \mod n$.*

Proof: *As $a \equiv b \mod n$ and $c \equiv d \mod n$, we can find $k_1, k_2 \in \mathbb{Z}$ with $a = b + k_1 n$ and $c = d + k_2 n$. Thus $a \pm c = b \pm d + n(k_1 \pm k_2)$ and $ac = bd + n(k_2 b + k_1 d)$. These equalities give (1), (2) and (3). Property (4) follows by successive application of (3), and (5) follows from (4).* □

Example 3.85. Find the remainder when 6^{1987} is divided by 37.

Solution:
$6^2 \equiv -1 \bmod 37$. Thus $6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \bmod 37$.

★**Exercise 3.86.** Prove that 7 divides $3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Example 3.87. Find the units digit of 7^{7^7}.

Solution: We must find $7^{7^7} \bmod 10$. Now, $7^2 \equiv -1 \bmod 10$, and so $7^3 \equiv 7^2 \cdot 7 \equiv -7 \equiv 3 \bmod 10$ and $7^4 \equiv (7^2)^2 \equiv 1 \bmod 10$. Also, $7^2 \equiv 1 \bmod 4$ and so $7^7 \equiv (7^2)^3 \cdot 7 \equiv 3 \bmod 4$, which means that there is an integer t such that $7^7 = 3+4t$. Upon assembling all this,

$$7^{7^7} \equiv 7^{4t+3} \equiv (7^4)^t \cdot 7^3 \equiv 1^t \cdot 3 \equiv 3 \mod 10.$$

Thus the last digit is 3.

Example 3.88. Prove that every year, including any leap year, has at least one Friday 13th.

Solution: It is enough to prove that each year has a Sunday the 1st. Now, the first day of a month in each year falls in one of the following days:

Month	Day of the year	mod7
January	1	1
February	32	4
March	60 or 61	4 or 5
April	91 or 92	0 or 1
May	121 or122	2 or 3
June	152 or 153	5 or 6
July	182 or183	0 or 1
August	213 or 214	3 or 4
September	244 or 245	6 or 0
October	274 or 275	1 or 2
November	305 or 306	4 or 5
December	335 or 336	6 or 0

(The above table means that, depending on whether the year is a leap year or not, that March 1st is the 60th or 61st day of the year, etc.) Now, each remainder class modulo 7 is represented in the third column, thus each year, whether leap or not, has at least one Sunday the 1st.

★**Exercise 3.89.** Prove that for any integer $k > 0$, $2^k - 5$ never leaves remainder 1 when divided by 7.

The proof of the following is left as an exercise. Recall that **iff** is shorthand for **if and only if**.

Theorem 3.90. $a \equiv b \pmod{n}$ *iff* $a \bmod n = b \bmod n$.

Example 3.91. Since $1961 \bmod 37 = 0$ and $356 \bmod 37 = 23$, and $0 \neq 23$, we know that $1961 \not\equiv 356 \pmod{37}$ by Theorem 3.90.

Note: *Our definition of* mod *requires that* $n > 0$ *and* $a \geq 0$. *It is possible to define* $a \bmod n$ *when* a *is negative. Unfortunately, there are two possible ways of doing so based on how you define the remainder when the dividend is negative. One possible answer is negative and the other is positive. They always differ by* n*, so computing one from the other is easy.*

Example 3.92. Since $-13 = (-2) * 5 - 3$ and $-13 = (-3) * 5 + 2$, we might consider the remainder of $-13/5$ as either -3 or 2. Thus, $-13 \bmod 5 = -3$ and $-13 \bmod 5 = 2$ both seem like reasonable answers. Fortunately, the two possible answers differ by 5. In fact, you can always obtain the positive possibility by adding n to the negative possibility.

★**Exercise 3.93.** Fill in the missing numbers that are congruent to 1 (mod 4) (listed in increasing order)

_____, -11, _____, -3, 1, 5, _____, _____, 17, _____

Definition 3.94. *Let* a*,* b *be integers with one of them different from* 0. *The* **greatest common divisor** d *of* a, b*, denoted by* $d = \gcd(a, b)$ *is the largest positive integer that divides both* a *and* b.

Example 3.95. Since $300 = 2^2 \cdot 3 \cdot 5^2$ and $70 = 2 \cdot 5 \cdot 7$, $\gcd(300, 70) = 2 \cdot 5 = 10$.

Factoring numbers in order to determine the greatest common divisor is inefficient. There is a better algorithm to compute it based on the fact (which we will not prove) that $\gcd(a, b) = \gcd(b, a \bmod b)$. Since $\gcd(a, b) = \gcd(b, a)$, we can assume that $a > b$ when we apply this rule. Further, once $a \bmod b = 0$, we will know that $\gcd(a, b) = b$.

Example 3.96. We can compute $\gcd(300, 70)$ as follows:

$$\begin{aligned} \gcd(300, 70) &= \gcd(70, 300 \bmod 70) = \gcd(70, 20) \\ &= \gcd(20, 70 \bmod 20) = \gcd(20, 10) \\ &= \gcd(10, 20 \bmod 10) = \gcd(10, 0) = 10. \end{aligned}$$

The following procedure is based on this idea.

Procedure 3.97. Euclid's Algorithm

```
// Given integers a and b, return their greatest common divisor
int gcd(a, b) {
    while (b!=0) {
        r = a mod b
        a=b
        b=r
    }
    return a
}
```

Example 3.98. We compute $\gcd(300, 70)$ again, this time explicitly using Euclid's algorithm.

step	a	b	r
1	300	70	20
2	70	20	10
3	20	10	0
4	10	0	0

Since $b = 0$, we can stop and we know that $\gcd(300, 70) = 10$.

★**Exercise 3.99.** Compute $\gcd(524, 118)$ using Euclid's algorithm.

Definition 3.100. *Two integers are said to be* **relatively prime** *if they have no factors in common. That is, a and b are relatively prime exactly when* $\gcd(a, b) = 1$.

Example 3.101. Since we previously saw that $\gcd(300, 70) = 10$, 300 and 7 are not relatively prime. On the other hand, 125 and 16 are relatively prime since they have no common factors ($125 = 5^3$ and $16 = 2^4$).

★**Exercise 3.102.** Determine whether or not 867 and 5309 are relatively prime by first using Euclid's algorithm to determine their gcd.

Definition 3.103. *The* **floor** *of a real number x, written $\lfloor x \rfloor$, is the largest integer that is less than or equal to x. The* **ceiling** *of a real number x, written $\lceil x \rceil$, is the smallest integer that is greater than or equal to x.*

Example 3.104. $\lfloor 4.5 \rfloor = 4$, $\lceil 4.5 \rceil = 5$, $\lfloor 7 \rfloor = \lceil 7 \rceil = 7$.
In general, if n is an integer, then $\lfloor n \rfloor = \lceil n \rceil = n$.

★**Exercise 3.105.** Determine each of the following.

1. $\lfloor 9.9 \rfloor =$ _____
2. $\lceil 9.9 \rceil =$ _____
3. $\lfloor 9.00001 \rfloor =$ _____
4. $\lceil 9.00001 \rceil =$ _____
5. $\lfloor 9 \rfloor =$ _____
6. $\lceil 9 \rceil =$ _____

The following Theorem and Corollary are somewhat obvious, but since floors and ceiling can trip people up, they are useful to have written down explicitly.

Theorem 3.106. *Let a be an integer and x be a real number. Then $a \leq x$ if and only if $a \leq \lfloor x \rfloor$.*

Proof: *If $a \leq \lfloor x \rfloor$, then $a \leq \lfloor x \rfloor \leq x$ is clear. On the other hand, assume $a \leq x$. Then a is an integer that is less than or equal to x. Since $\lfloor x \rfloor$ is the largest integer that is less than or equal to x, $a \leq \lfloor x \rfloor$.* □

Corollary 3.107. *Let a, b, and c be integers. Then $a \leq b/c$ if and only if $a \leq \lfloor b/c \rfloor$.*

Proof: *Since b/c is a real number, this is a special case of Theorem 3.106.* □

3.3 Functions

This section is meant as a review of what you hopefully already learned in an earlier course, probably in high school. Thus, it is pretty brief. But we do try to cover all of the important material and provide enough examples to illustrate the concepts.

3.3.1 Definitions

Definition 3.108. *Let A and B be sets. Then a* **function** *f from A to B assigns to each element of A exactly one element from B. We write $f : A \to B$ if f is a function from A to B. If $a \in A$ and f assigns to a the value $b \in B$, we write $f(a) = b$. We also say that f* **maps** *a to b.*

If $A = B$, we sometimes say f is a function **on** *A.*

Example 3.109. If $A = B = \mathbb{N}$, we can define a function $f : A \to B$ by $f(x) = x^2$. Then $f(1) = 1$, $f(2) = 4$, $f(3) = 9$, etc. Although $f(x)$ is defined for all $x \in A$, not every $b \in B$ is mapped to by f. For instance, there is no $a \in A$ for which $f(a) = 5$.

Example 3.110. Notice that we can define $f(x) = \sqrt{x}$ on the positive real numbers, but we *cannot* define it on the positive integers since $\sqrt{2}$ is not an integer. Similarly, since $\sqrt{-1} = i \notin \mathbb{R}$, we cannot define it on the real numbers. We *can* let it be a function from $\mathbb{R}$ to $\mathbb{C}$, though. But we won't because this course is complex enough even without complex numbers.

Definition 3.111. *Let f be a function from A to B.*

1. *We call A the* **domain** *of f.*
2. *We call B the* **codomain** *of f.*
3. *The* **range** *of f is the set $\{b | f(a) = b \text{ for some } a \in A\}$. In other words the range is the subset of B that are actually mapped to by f.*

Example 3.112. Let $A = B = \mathbb{N}$ and $f : A \to B$ be defined by $f(x) = x^2$. Then the domain and codomain of f are both $\mathbb{N}$, and the range is $\{a^2 | a \in \mathbb{N}\}$, which is a proper subset of the codomain.

Figure 3.3 gives a pictorial representation of a function. Notice that in this example every element in A has precisely one arrow going from it. So if I ask "what is $f(x)$?", there is always an answer and it is always unique. On the other hand, there is a point in B that has two arrows going to it and several points that have no arrows going to them. This is fine.

Figure 3.4 does not represent a function since there are several points in A which have two arrows going from them and several with no arrows at all. The problem here is that if I ask "what is $f(x)$?", sometimes there is no answer and sometimes there are multiple answers. Thus, f would not represent a function.

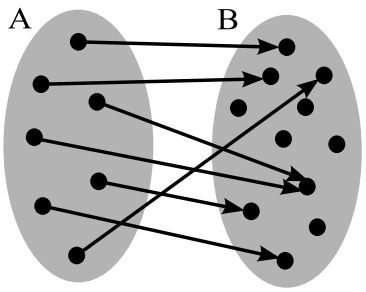


Figure 3.3: Pictorial representation of a function from A to B.

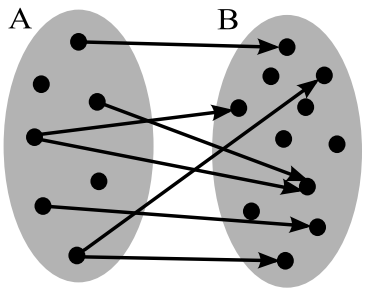


Figure 3.4: This picture does *not* represent a function.

Note: *In figures 3.3 and 3.4, the dots represent all of the elements of the sets A and B and the gray ovals are mainly there to help identify which dots are in which set. However, in these sorts of diagrams it is more common for the dots to represent only* some *of the elements. You need to let the context help you determine how to properly interpret these diagrams.*

Example 3.113. Give a formal definition of a function that assigns to an age the number of complete decades someone of that age has lived. For instance, $f(34) = 3$ and $f(5) = 0$. Be sure to indicate what the domain and codomain are.

Solution: It isn't hard to see that the domain and codomain are both $\mathbb{N}$. Thus we want a function $f : \mathbb{N} \to \mathbb{N}$. One way to define f is by $f(x) = \lfloor x/10 \rfloor$.

★**Exercise 3.114.** Give a formal definition of a function that returns the parity of an integer. That is, it returns 0 for even numbers and 1 for odd numbers. Be sure to indicate what the domain and codomain are.

Answer _____

_____

Definition 3.115. *Let $f : A \to B$ be a function.*

- *f is said to be* **injective** *or* **one-to-one** *if and only if $f(a) = f(b)$ implies that $a = b$. In other words, f maps every element of A to a* different *element of B.*
- *f is said to be* **surjective** *or* **onto** *if and only if for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$. In other words, every element in B gets mapped to by some element in A.*
- *f is said to be* **bijective** *or a* **one-to-one correspondence** *if it is both injective and surjective.*

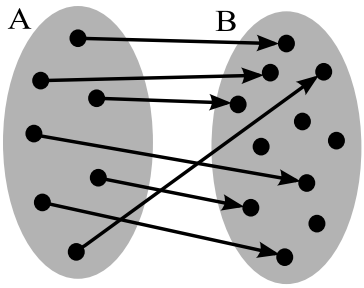


Figure 3.5: Pictorial representation of a *one-to-one* function.

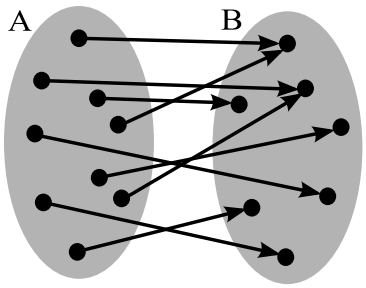


Figure 3.6: Pictorial representation of an *onto* function.

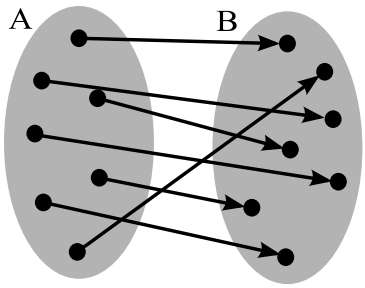


Figure 3.7: Pictorial representation of an *bijective* function.

Example 3.116. For each of the following functions from $\mathbb{Z}$ to $\mathbb{Z}$, we determine whether or not they are one-to-one and onto.

(a) Let $f(x) = x + 2$. Notice that if $f(a) = f(b)$, then $a + 2 = b + 2$ so $a = b$. Thus, f is one-to-one. Also notice that for any $b \in \mathbb{Z}$, $f(b - 2) = b - 2 + 2 = b$, so f is onto.

(b) Let $g(x) = x^2$. Since $g(1) = g(-1) = 1$, g is not one-to-one. Also notice that there is no integer a such that $g(a) = a^2 = 5$, so g is not onto.

(c) Let $h(x) = 2x$. If $h(a) = h(b)$, then $2a = 2b$ so $a = b$. Thus, h is one-to-one. But there is no integer a such that $h(a) = 2a = 3$, so a is not onto.

(d) Let $r(x) = \lfloor x/2 \rfloor$. Notice that $r(0) = \lfloor 0/2 \rfloor = \lfloor 0 \rfloor = 0$ and $r(1) = \lfloor 1/2 \rfloor = \lfloor 0 \rfloor = 0$, so r is not one-to-one. But for any integer b, $r(2b) = \lfloor 2b/2 \rfloor = \lfloor b \rfloor = b$, so r is onto.

The functions in the previous exercise were specifically chosen to demonstrate that all four possibilities of being or not being one-to-one and onto (one-to-one and onto, one-to-one and not onto, not one-to-one but onto, and not one-to-one or onto) are possible.

The following theorem should come as no surprise if you take a few minutes to think about it (and you *should* take a few minutes to think about it until you are convinced it is correct).

Theorem 3.117. *Let $f : A \to B$ be a function, and let A and B be finite.*

1. *If f is one-to-one, then $|A| \leq |B|$.*
2. *If f is onto, then $|A| \geq |B|$.*
3. *If f is bijective, then $|A| = |B|$.*

★**Exercise 3.118.** Let's test your understanding of the material so far. Answer each of the following true/false questions, giving a very brief justification/counterexample.

(a) ___If $f : A \to B$ is onto, then the domain and range are not only the same size, but they are the same set.

(b) ___If $f : A \to A$, then f must be one-to-one and onto.

(c) ___If $f : A \to B$ is both one-to-one and onto, then A and B have the same number of elements.

(d) ___Let $f(1) = 2$ and $f(1) = 3$. Then f is a valid function.

(e) ___Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3$. Then f is one-to-one and onto.

(f) ___Let $f : \mathbb{R}^+ \to \mathbb{R}$ be defined by $f(x) = \sqrt{x}$. Then f is a function that is neither one-to-one nor onto.

(g) ___The range of a function is always a subset of the codomain.

(h) ___A function that is one-to-one is guaranteed to be onto.

(i) ___Let $a, b \in \mathbb{Z}$, with $a \neq 0$, and define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = ax + b$. Then f is one-to-one and onto.

(j) ___Let $a, b \in \mathbb{Z}$, with $a \neq 0$, and define $f : \mathbb{N} \to \mathbb{N}$ by $f(x) = ax + b$. Then f is one-to-one and onto.

(k) ___Let $a, b \in \mathbb{R}$, with $a \neq 0$, and define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$. Then f is one-to-one and onto.

Definition 3.119. *Let f be a one-to-one correspondence from A to B. The* **inverse** *of f, denoted by f^{-1}, is the function such that $f^{-1}(b) = a$ whenever $f(a) = b$.*
A function that has an inverse is called **invertible**. *Said another way, a function is* **invertible** *if and only if it is one-to-one and onto.*

Note: *It is important to note that the function f^{-1} is not the same thing as $1/f$. This is an unfortunate case when a notation can be interpreted in two different ways. That is, in some cases, a^{-1} means the inverse function and in other cases it means $1/a$. Usually the context will help you determine which one is the correct interpretation.*

Procedure 3.120. *One method of finding the inverse of a function is to replace $f(x)$ (or whatever the name of the function is) with y and solve for x (or whatever the variable is). Finally, replace y with x and you have the inverse. However, it is important to note that this only works if f is a one-to-one correspondence, so you typically need to verify that first.*

Example 3.121. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x + 2$. Notice that f is a one-to-one correspondence, so it has an inverse. We let $y = x + 2$. Solving for x, we get $x = y - 2$. Thus, $f^{-1}(x) = x - 2$.

Example 3.122. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Then f does not have an inverse since it is not one-to-one.

Example 3.123. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3$. We leave it to the reader to prove that f is one-to-one and onto. Given that, we can find it's inverse.

Let $y = x^3$. Taking the third root of both sides, we obtain $\sqrt[3]{y} = \sqrt[3]{x^3} = x$. Or $x = \sqrt[3]{y}$. Thus, the inverse of f is given by $f^{-1}(x) = \sqrt[3]{x}$.

Notice that the previous example works because $\sqrt[3]{x^3} = x$ (similarly for any odd power). However, it does *not* work for squares since $\sqrt{x^2} = |x|$ (similar for any even power). The fact that the absolute value shows up should clue you into the fact that x^2 is not one-to-one, so it can't be invertible.

★**Exercise 3.124.** Let $f(x) = 7x + 2$ be a function over $\mathbb{R}$. You can assume that f is a one-to-one correspondence. Find f^{-1}.

Definition 3.125. *Let g be a function from A to B and f a function from B to C. The* **composition** *of f and g, denoted by $f \circ g$, is defined as $(f \circ g)(x) = f(g(x))$ for any $x \in A$.*

In other words, to compose f with g, we *first* compute $g(x)$. Then we plug in $g(x)$ into the formula for f.

Note: *Look closely at the notation. $f \circ g$ has f before g, so it might seem like it should be $g(f(x))$–in other words, apply f first, then then g. But that is* not *how it is defined.*

Also notice that to compose f with g, it is necessary that the range of g is a subset of the domain of f since otherwise it would be impossible to compute.

Example 3.126. Let f and g be functions on $\mathbb{Z}$ defined by $f(x) = x^2$ and $g(x) = 2x - 5$. Compute $f \circ g$ and $g \circ f$, simplifying your answers.

Solution:

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = f(2x-5) = (2x-5)^2 = 4x^2 - 20x + 25.\\ (g \circ f)(x) &= g(f(x)) = g(x^2) = 2x^2 - 5.\end{aligned}$$

Notice that in the previous example, $f \circ g \neq g \circ f$. In other words, the order in which we compose functions matters since the result usually not the same (although occasionally it is).

★**Exercise 3.127.** Let f and g be functions on $\mathbb{R}$ defined by $f(x) = \lfloor x \rfloor$ and $g(x) = x/2$. Compute $f \circ g$ and $g \circ f$, simplifying your answers.

$(f \circ g)(x) =$ _____

$(g \circ f)(x) =$ _____

Definition 3.128. *We define the* **identity function**, *$\iota_A : A \to A$, by $\iota_A(x) = x$.*
The subscript can be omitted if the domain/codomain is clear.

Theorem 3.129. *Let f be an invertible function from A to B. Then $f \circ f^{-1} = \iota_B$ and $f^{-1} \circ f = \iota_A$.*

Proof: *Let $a \in A$ and define $b = f(a)$. Then by definition, $f^{-1}(b) = a$, so $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$. Thus, $f^{-1} \circ f = \iota_A$.*

Conversely, if $b \in B$ and we define $a = f^{-1}(b)$, then $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$. Thus, $f \circ f^{-1} = \iota_B$. □

Example 3.130. Prove or disprove that $f(x) = 2x + 1$ and $g(x) = 2x - 1$, defined over the real numbers, are inverses.

Solution: Notice that $(f \circ g)(x) = f(2x - 1) = 2(2x - 1) + 1 = 4x - 1 \neq x$. According to Theorem 3.129, this implies that f and g are not inverses.

★**Exercise 3.131.** Let's test your understanding of the material so far. Answer each of the following true/false questions, giving a very brief justification/counterexample.

(a) ___Let $a, b \in \mathbb{Z}$, with $a \neq 0$, and define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = ax + b$. Then f is invertible.

(b) ___Let $a, b \in \mathbb{Z}$, with $a \neq 0$, and define $f : \mathbb{N} \to \mathbb{N}$ by $f(x) = ax + b$. Then f is invertible.

(c) ___Let $a, b \in \mathbb{R}$, with $a \neq 0$, and define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$. Then f is invertible.

(d) ___If $f(x) = x^2$, then $f^{-1}(x) = 1/x^2$.

(e) ___Let n be a positive integer. Then the function $\sqrt[n]{x}$ is invertible on $\mathbb{R}$.

(f) ___Let n be a positive integer. Then the function $\sqrt[n]{x}$ is invertible on $\mathbb{N}$.

(g) ___Let n be a positive integer. Then the function $\sqrt[n]{x}$ is invertible on $\mathbb{R}^+$ (the positive real numbers).

(h) ___Let f and g be functions on $\mathbb{Z}^+$ defined by $f(x) = x^2$ and $g(x) = 1/x$. Then $f \circ g = g \circ f$.

(i) ___Let f and g be functions on $\mathbb{Z}$ defined by $f(x) = (x + 1)^2$ and $g(x) = x + 1$. Then $f \circ g = g \circ f$.

(j) ___Let $f(x) = \lfloor x \rfloor$ and $g(x) = \lceil x \rceil$ be defined on the real numbers. Then $f \circ g = g \circ f$.

(k) ___Let $f(x) = \lfloor x \rfloor$ and $g(x) = \lceil x \rceil$ be defined on the real numbers. Then f and g are inverses of each other.

(l) ___Let $f(x) = x^2$ and $g(x) = \sqrt{x}$ be defined over the positive real numbers. Then f and g are inverses of each other.

3.3.2 Function Proofs

In this section we give more in depth examples of proving things about functions.

Procedure 3.132. *To show that a function f is one-to-one, you just need to show that whenever $f(a) = f(b)$, then $a = b$.*

Example 3.133. Let $f(x) = 2x - 3$ be a function on the integers. Show that f is one-to-one.

Solution: Let $a, b \in \mathbb{Z}$ and assume that $f(a) = f(b)$. Then $2a - 3 = 2b - 3$. Adding 3 to both sides, we get $2a = 2b$. Dividing both sides by two, we obtain $a = b$. Therefore, $f(x) = 2x - 3$ is one-to-one.

★**Question 3.134.** Previously we mentioned that 'working both sides' was not an appropriate proof technique. Why is it O.K. in the previous example?

Answer _____

_____

★**Exercise 3.135.** Prove that $f(x) = 5x$ is one-to-one over the real numbers.

Proof _____

_____

_____

Procedure 3.136. *To show that a function f is* **not** *one-to-one, we simply need to find two values $a \neq b$ in the domain such that $f(a) = f(b)$. That is, we just need to show that there are two different numbers in the domain that are mapped to the same value in the codomain.*

Example 3.137. Let $f(x) = x^2$ be a function on the integers. Show that f is not one-to-one.

Solution: Notice that $f(-1) = f(1) = 1$. Thus, $f(x)$ is not one-to-one.

★**Exercise 3.138.** Let $f(x) = \lfloor x \rfloor$ be a function on $\mathbb{R}$. Prove that f is not one-to-one.

Proof _____

_____

Procedure 3.139. *To show that a function f is onto, we need to show that for an arbitrary $b \in B$, there is some $a \in A$ such that $f(a) = b$. That is, show that every value in B is mapped to by f.*

Example 3.140. Let $f(x) = x^3$ be a function on the real numbers. Show that f is onto.

Solution: Let $b \in \mathbb{R}$. Then $f\left(\sqrt[3]{b}\right) = \left(\sqrt[3]{b}\right)^3 = b^{3/3} = b$. Since every $b \in \mathbb{R}$ is mapped to (from $\sqrt[3]{b}$), f is onto.

★**Exercise 3.141.** Let $f(x) = 2x + 1$ be a function on $\mathbb{R}$. Show that f is onto.

Proof _____

_____

_____

_____

Procedure 3.142. *To show that a function f is* **not** *onto, we just need to find some $b \in B$ such that there is no $a \in A$ with $f(a) = b$. In other words, we just need to find one value that isn't mapped to by f.*

Example 3.143. Let $f(x) = x^3$ be a function on the integers. Show that f is not onto.

Solution: There is no integer a such that $a^3 = 2$. In other words, 2 is not mapped to. Thus, $f(x)$ is not onto.

★**Exercise 3.144.** Let $f(x) = \lfloor x \rfloor$ be a function on $\mathbb{R}$. Prove that f is not onto.

Proof _____

_____

It is important to remember that whether or not a function is one-to-one or onto might depend on the domain/codomain over which the function is defined. For instance, notice that in the last two examples we used the same function but on different domains/codomains. In one case the function was onto, and in the other case it wasn't.

★**Exercise 3.145.** Consider the function $f(x) = x^2$.

(a) Prove or disprove that $f(x) = x^2$ is one-to-one on $\mathbb{Z}$.

Answer

(b) Prove or disprove that $f(x) = x^2$ is one-to-one on $\mathbb{R}$.

Answer

(c) Prove or disprove that $f(x) = x^2$ is one-to-one on $\mathbb{N}$.

Answer

★**Exercise 3.146.** Let $f(x) = 3x - 5$ be a function over $\mathbb{R}$. Prove that f has an inverse and then find it.

★**Exercise 3.147.** Determine which of the following functions from $\mathbb{Z}$ to $\mathbb{Z}$ is one-to-one and/or onto. Prove your answers.

(a) $f(x) = x - 7$

Answer

(b) $g(x) = x^4$

Answer

(c) $h(x) = 3x$

Answer

(d) $r(x) = \lfloor x/2 \rfloor$

Answer

Example 3.148. Let f be a function from B to C, and g be a function from A to B. If both f and g are one-to-one, prove that $f \circ g$ is one-to-one.

Direct Proof:

For any distinct elements $x, y \in A$, $g(x) \neq g(y)$, since g is one-to-one. Since f is also one-to-one, then $f(g(x)) \neq f(g(y))$, which is the same as $(f \circ g)(x) \neq (f \circ g)(y)$. Therefore $f \circ g$ is one-to-one. □

Proof by Contradiction:

Assume $f \circ g$ is not one-to-one. Then there exist distinct elements $x, y \in A$ such that $(f \circ g)(x) = (f \circ g)(y)$. This is equivalent $f(g(x)) = f(g(y))$. Since f is one-to-one, it must be the case that $g(x) = g(y)$. But $x \neq y$, and g is one-to-one, so $g(x) \neq g(y)$. This is a contradiction. Therefore $f \circ g$ is one-to-one. □

3.4 Partitions and Equivalence Relations

Partitions and equivalence relations are not only fun and interesting to learn about, they have various applications, including some related to software testing that we will explore later.

Definition 3.149. *Let $S \neq \varnothing$ be a set. A* **partition** *of S is a collection of non-empty, pairwise disjoint subsets of S whose union is S.*

Example 3.150. Define $\mathbb{E} = \{2k : k \in \mathbb{Z}\}$ and $\mathbb{O} = \{2k+1 : k \in \mathbb{Z}\}$. Clearly $\mathbb{E}$ is the set of even integers and $\mathbb{O}$ is the set of odd integers. Since $\mathbb{E} \cap \mathbb{O} = \varnothing$ and $\mathbb{E} \cup \mathbb{O} = \mathbb{Z}$, $\{\mathbb{E}, \mathbb{O}\}$ is a partition of $\mathbb{Z}$. Put another way, we can partition the integers based on parity.

Example 3.151. We can partition the socks in our sock drawer by color. In other words, we put all of the black socks in one set, the white ones in another, the green ones in another, etc. For simplicity, we can put all of the multi-color socks in a single set.

Example 3.152. We can partition the set of all humans by putting each person into a set based on the first letter of their first name. So *Adam* and *Adele* go into set A and *Zeek* goes into set Z, for instance. The sets in the partition are $A, B, \ldots Z$.[a]

[a] For simplicity, we assume everyone's name is written using the Roman alphabet.

Example 3.153. Let $A = \{1, 5, 8\}$, $B = \{2, 3\}$, $C = \{4\}$, $D = \{6, 9\}$, and $E = \{7, 10, 11, 12\}$. Then the sets A, B, C, D, and E form a partition of the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

★**Exercise 3.154.** You must decide on test cases for a method `int maximum(int a,int b)` that returns the maximum of its arguments. How would you partition the possible inputs into sets such that if it is correct for one (or a few) tests of cases from that set, it is probably correct for the rest of the cases in that set? Notice that the set of inputs is $\mathbb{Z} \times \mathbb{Z}$.

Answer _____

_____

_____

Most of the partitions we talk about will be based on some meaningful characteristic of the elements of a set–like parity, color, or sign. But this is not inherent in the definition. For instance, the sets in the partition from Example 3.153 do not seem to have any significant meaning. Some, like the one in Example 3.150, will have a precise mathematical definition. Others, like the one in Examples 3.151 will not.

★**Exercise 3.155.** Define a partition on $\mathbb{Z}$ that contains more than one subset.

Answer _____

_____

_____

Example 3.156. Let $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$, $3\mathbb{Z}+1 = \{3k+1 : k \in \mathbb{Z}\}$, and $3\mathbb{Z}+2 = \{3k+2 : k \in \mathbb{Z}\}$.[a] Since

$$(3\mathbb{Z}) \cup (3\mathbb{Z}+1) \cup (3\mathbb{Z}+2) = \mathbb{Z} \text{ and}$$

$$(3\mathbb{Z}) \cap (3\mathbb{Z}+1) = \varnothing,\ (3\mathbb{Z}) \cap (3\mathbb{Z}+2) = \varnothing, (3\mathbb{Z}+1) \cap (3\mathbb{Z}+2) = \varnothing,$$

$\{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$ is a partition of $\mathbb{Z}$.

[a] The notation in this example may seem a bid odd at first. How are you supposed to interpret "$3\mathbb{Z}+1$"? Is this 3 times the set $\mathbb{Z}$ plus 1? What does it mean to do algebra with sets and numbers? I won't get into all of the technical details, but here is a short answer. You can think of "$3\mathbb{Z}+1$" as just a name. Sure, it may seem like an odd name, but why can't we name a set whatever we want? Some people name their kids *Jon Blake Cusack 2.0* and get away with it. You can also think of "$3\mathbb{Z}+1$" as describing how to create the set—by taking every element from $\mathbb{Z}$, multiplying it by 3, and then adding 1. Thus, you can think of "$3\mathbb{Z}+1$" as being both an algebraic expression and a name.

★**Exercise 3.157.** Let $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ (the set of irrational numbers). Prove that $\{\mathbb{Q}, \mathbb{I}\}$ is a partition of $\mathbb{R}$.

Proof _____

_____

_____

Recall that when a list of number is given between parentheses (e.g. $(1,2,3)$), it typically denotes an ordered list. That is, the order that the element are listed matters. So, for instance, $(1,2)$ and $(2,1)$ are not the same thing.

Next we will develop an alternative way of thinking about partitions: equivalence relations. After defining some terms and providing a few examples, we will make the connection between partitions and equivalence relations more clear.

Definition 3.158. *Let A, B be sets. A* **relation** *(or* **binary relation***) from A to B is a subset of the Cartesian product $A \times B$.*

Given a relation R, we say that x is **related to** *y if $(x,y) \in R$. We sometimes write this as xRy. An alternative notation is $x \sim y$.*

If R is a relation from A to A, we sometimes say R is a relation **on** *A.*

Example 3.159. Let A be the set of all students at this school and B be the set of all courses at this school. We can define a relation R by saying that xRy if student x has taken course y. Said another way, we can define R by saying that $(x, y) \in R$ if student x has taken course y.

Example 3.160. We can define a relation $R = \{(a, a^2) : a \in \mathbb{Z}\}$. That is, x is related to y if $y = x^2$.

Example 3.161. We can define a relation on $\mathbb{Z}$ by saying that x is related to y if they have the same parity. Thus, $(2, 0)$, $(234, -342)$, $(3, 17)$ are all in R, but $(2, 127)$ is not.

★**Question 3.162.** Define $R = \{(a, b) : a, b \in \mathbb{Z} \text{ and } a < b\}$. Is R a relation? Explain.

Answer _____

_____

★**Question 3.163.** Is $\{(1, 2), (345, 7), (43, 8675309), (11, 11)\}$ a relation on $\mathbb{Z}^+$? Explain.

Answer _____

_____

Definition 3.164. *A relation R on set A is said to be* **reflexive** *if for all $x \in A$, xRx (or $(x, x) \in R$).*

★**Exercise 3.165.** Let P be the set of all people. Which of the following relations on P are reflexive? Explain why or why not.

(a) $T = \{(a, b) : a, b \in P \text{ and } a \text{ is taller than } b\}$

(b) N is the relation with a related to b iff a's name starts with the same letter as b's name.

(c) C is the relation defined by $(a, b) \in C$ if a and b have been to the same city.

(d) $K = \{(a, b) : a, b \in P \text{ and } a \text{ does not know who } b \text{ is}\}$

(e) $R = \{(\text{Barack Obama}, \text{George W. Bush})\}$.

(a) T: _____

_____

(b) N: _____

_____

(c) C: _____

_____

(d) K: _____

_____

(e) R: _____

_____

Definition 3.166. *A relation R on set A is said to be* **symmetric** *if for all $x, y \in A$, xRy implies yRx (or $(x, y) \in R$ implies $(y, x) \in R$).*

★**Exercise 3.167.** Which of the relations from Example 3.165 are symmetric? Explain why or why not.

(a) T: _____

_____

(b) N: _____

_____

(c) C: _____

_____

(d) K: _____

(e) R: _____

Definition 3.168. *A relation R on set A is said to be* **anti-symmetric** *if for all $x, y \in A$, xRy and yRx implies $x = y$ (or $(x, y) \in R$ and $(y, x) \in R$ implies $x = y$).*

★**Question 3.169.** Let R be a relation on $\mathbb{Z}$.

(a) If $(1, 1) \in R$, can you tell whether or not R is anti-symmetric? Explain.

Answer _____

(b) What if $(1, 2)$ and $(2, 1)$ are both in R? Can you tell whether or not R is anti-symmetric?

Answer _____

★**Question 3.170.** An alternative definition of *anti-symmetric* is that if $x \neq y$, then (x, y) and (y, x) are not both in the relation. Why is this definition equivalent?

Answer _____

Note: *The definition of anti-symmetric is sometimes misunderstood. Let's call elements of the form (x, x)* **diagonal** *elements and elements of the form (x, y) where $x \neq y$* **off-diagonal** *elements.*[a] *Then the definition of anti-symmetric is only dealing with off-diagonal elements. It is saying nothing about the diagonal elements. In other words, it is* **not** *saying that $(x, x) \in R$ for any, let alone all, values of x. But it also isn't saying $(x, x) \notin R$. It is simply saying that the* only *way for both (x, y) and (y, x) to be in R is if $x = y$.*

The alternative definition given in the previous question may help a little. Notice that the definition there starts with 'if $x \neq y$...' So what does the definition say about the case $x = y$? Nothing. It never mentions it.

You could redefine it as follows: R is anti-symmetric if for all non-diagonal elements $(x, y) \in R$, $(y, x) \notin R$. But that can be problematic if you forget that $x \neq y$ is required.

[a] These terms come from thinking about the elements of a relation as elements in a matrix indexed by the

members of the set. If this doesn't make sense, don't worry too much about it.

★**Exercise 3.171.** Which of the relations from Example 3.165 are anti-symmetric? Explain why or why not.

(a) T: _____

_____

(b) N: _____

_____

(c) C: _____

_____

(d) K: _____

_____

(e) R: _____

_____

★**Question 3.172.** Answer each of the following. Include a brief justification/example.

(a) If a relation is not symmetric, is it anti-symmetric?

Answer _____

_____

(b) If a relation is not anti-symmetric, is it symmetric?

Answer _____

_____

(c) Can a relation be both symmetric and anti-symmetric?

Answer

★**Exercise 3.173.** Give an example of a relation on any set of your choice that is both symmetric and anti-symmetric. Justify your answer.

Answer

Definition 3.174. *A relation R on set A is said to be* **transitive** *if for all $x, y, z \in A$, xRy and yRz implies xRz (or $((x, y) \in R$ and $(y, z) \in R)$ implies $(x, z) \in R$).*

★**Exercise 3.175.** Which of the relations from Example 3.165 are transitive? Explain why or why not.

(a) T:

(b) N:

(c) C:

(d) K:

(e) R:

Definition 3.176. *A relation which is reflexive, symmetric and transitive is called an* **equivalence relation**.

Example 3.177. Let $S = \{\text{All Human Beings}\}$, and define the the relation M by $(a, b) \in M$ if a has the same (biological) mother[a] as b. Show that M is an equivalence relation.

Proof: (**Reflexive**) a has the same mother as a, so $(a, a) \in M$ and M is reflexive.

(**Symmetric**) If a has the same mother as b, then b clearly has the same mother as a. Thus, $(a, b) \in M$ implies $(b, a) \in M$, so M is symmetric.

(**Transitive**) If a has the same mother as b, and b has the same mother as c, then clearly a has the same mother as c. In other words, $(a, b) \in M$ and $(b, c) \in M$ implies that $(a, c) \in M$, so M is transitive.

Since M is reflexive, symmetric, and transitive, it is an equivalence relation. □

[a] The important assumption we are making is that each person has exactly one mother.

★**Exercise 3.178.** Which of the relations from Example 3.165 are equivalence relations? Explain why or why not.

(a) T: _____

_____

(b) N: _____

_____

(c) C: _____

_____

(d) K: _____

_____

(e) R: _____

_____

Definition 3.179. *A relation which is reflexive, anti-symmetric and transitive is called a* **partial order**.

★**Exercise 3.180.** Which of the relations from Example 3.165 are partial orders? Explain why or why not.

(a) T: _____

_____

(b) N: _____

_____

(c) C: _____

_____

(d) K: _____

_____

(e) R: _____

_____

★**Exercise 3.181.** Let X be a collection of sets. Let R be the relation on X such that A is related to B if $A \subseteq B$. Prove that R is a partial order on X.

Proof: (**Reflexive**) _____

(**Anti-symmetric**) _____

_____

(**Transitive**) _____

□

Labeling the lines of these proofs with what property we are proving isn't strictly necessary. However, it does make the proofs a little easier to read.

★**Exercise 3.182.** Consider the relation $R = \{(1,2),(1,3),(1,5),(2,2),(3,5),(5,5)\}$ on the set $\{1,2,3,4,5\}$. Prove or disprove each of the following.

(a) R is reflexive

Answer

(b) R is symmetric

Answer

(c) R is anti-symmetric

Answer

(d) R is transitive

Answer

(e) R is an equivalence relation

Answer

(f) R is a partial order

Answer

Next we show that congruence modulo n (See Definition 3.79) is an equivalence relation.

Theorem 3.183. *Let n be a positive integer. Let R be the relation on the set of integers defined by $R = \{(a, b) : a \equiv b \pmod{n}\}$. Then R is an equivalence relation.*

Proof: *We need to show that R is reflexive, symmetric, and transitive.*

*(**Reflexive**) Clearly $a - a = 0 \cdot n$, so $a \equiv a \pmod{n}$. Thus, R is reflexive.*

*(**Symmetric**) Assume $(a, b) \in R$. Then $a \equiv b \pmod{n}$, which implies $a - b = kn$ for some integer k. So $b - a = (-k)n$, and since $-k$ is an integer, $b \equiv a \pmod{n}$. Therefore, $(b, a) \in R$. Thus, R is symmetric.*

*(**Transitive**) Assume $(a, b), (b, c) \in R$. Then $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Thus, $a - b = kn$ for some integer k and $b - c = ln$ for some integer l. Given these, we can see that*

$$a - c = (a - b) + (b - c) = kn + ln = (k + l)n.$$

Since $k + l$ is an integer, $a \equiv c \pmod{n}$. Thus $(a, c) \in R$, so R is transitive. □

Notice that if we let $n = 2$ in the previous theorem, we essentially have the relation from Example 3.161.

★**Fill in the details 3.184.** Let R be the relation on the set of ordered pairs of positive integers (that is, $\mathbb{Z}^+ \times \mathbb{Z}^+$) such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.[a]

Proof: We need to show that R is reflexive, symmetric, and transitive.

(**Reflexive**) Since $ab = ba$ for all positive integers, _____ $\in R$ for all (a, b). Thus R is reflexive.

(**Symmetric**) Assume $((a, b), (c, d)) \in R$. Then we know that $ad =$ _____.

We can rearrange this as $cb =$ _____. Thus, _____ $\in R$, so R is

_____.

(**Transitive**) Assume that $((a, b), (c, d)) \in R$ and $((c, d), (e, f)) \in R$. Then we

know that _____ and _____. Solving the sec-

ond for c, we get $c =$ _____. Plugging it into the first we get $ad =$

_____. Multiplying both sides by f, and canceling the d on both sides

yields _____. Thus, _____ $\in R$, so R is transitive.

□

[a] In this example, R is a relation on a set of ordered pairs. Thus, the elements of R are ordered pairs of ordered pairs. Don't let this confuse you. The elements of a relation are always ordered pairs. What each part

of the pair is depends on the underlying set. If it is the set of animals, then the elements of the relation are ordered pairs of animals. If it is $\mathbb{Z}$, then the elements of the relation are ordered pairs of integers. And if it is $\mathbb{Z}^+ \times \mathbb{Z}^+$, then the elements of the relation are ordered pairs of ordered pairs of positive integers.

Definition 3.185. *Let R be an equivalence relation on a set S. Then the* **equivalence class of a**, *denoted by* **$[a]$**, *is the subset of S containing all of the elements that are related to a. More formally,*

$$[a] = \{x \in S : xRa\}.$$

If $x \in [a]$, we say that x is a **representative** *of the equivalence class $[a]$. Note that* any *element of an equivalence class can serve as a representative.*

Example 3.186. The equivalence class of 3 modulo 8 is $[3] = \{8k + 3 : k \in \mathbb{Z}\}$. Notice that $[11] = \{8k + 11 : k \in \mathbb{Z}\} = \{8k + 3 : k \in \mathbb{Z}\} = [3]$. In fact, $[3] = [8l + 3]$ for all integers l. In other words, any element of the form $8l + 3$, where l is an integer, can serve as a representative of [3]. Further, we can call this class [3], [11], [19], etc. It doesn't really matter since they all represent the same set of integers. Of course, [3] is the most logical choice.

Example 3.187. Notice that if our relation is congruence modulo 3, we can define three equivalence classes:

$$\begin{aligned} [0] &= \{3k : k \in \mathbb{Z}\}, \\ [1] &= \{3k + 1 : k \in \mathbb{Z}\}, \text{ and} \\ [2] &= \{3k + 2 : k \in \mathbb{Z}\}. \end{aligned}$$

It isn't too difficult to see that $\mathbb{Z} = [1] \cup [2] \cup [3]$, and that these three sets are disjoint. In other words, the equivalence classes $\{[1], [2], [3]\}$ form a partition of $\mathbb{Z}$. As we will see shortly, this is not a coincidence.

Lemma 3.188. *Let R be an equivalence relation on a set S. Then two equivalence classes are either identical or disjoint.*

> **Proof:** *Let $a, b \in S$, and assume $[a] \cap [b] \neq \varnothing$ (that is, that they are not disjoint). We need to show that $[a] = [b]$. First, let $x \in [a] \cap [b]$ (which exists since $[a] \cap [b] \neq \varnothing$). Then xRa and xRb, so by symmetry aRx and by transitivity aRb.*
>
> *Now let $y \in [a]$. Then yRa. Since we just showed that aRb, then yRb by transitivity. Thus $y \in [b]$. Therefore $[a] \subseteq [b]$.*
>
> *A symmetric argument proves that $[b] \subseteq [a]$. Therefore, $[a] = [b]$.* □

Let's bring together some of the examples of partitions with examples of equivalence relations and classes.

Example 3.189. We just saw that congruence modulo 3 is an equivalence relation with three equivalence classes, $\{3k : k \in \mathbb{Z}\}$, $\{3k+1 : k \in \mathbb{Z}\}$, and $\{3k+2 : k \in \mathbb{Z}\}$. In Example 3.156, we defined a partition of $\mathbb{Z}$ using these same three subsets.

Example 3.190. In Example 3.161 we defined a relation on $\mathbb{Z}$ based on parity. It is not difficult to see that the equivalence classes of that relation are $[0] = \mathbb{E}$ and $[1] = \mathbb{O}$. Notice these are the same subsets we used to partition $\mathbb{Z}$ in Example 3.150.

Example 3.191. In Example 3.152 we defined a partition of people according to the first letter of their first name. The sets in the partition were $A, B, \ldots, Z$.

We can define an equivalence relation on the set of all people by saying a is related to b if a's name starts with the same letter of the alphabet as b's name. In a series of previous exercises, you proved that this defines an equivalence relation. Notice that the equivalence classes are the sets $A, B, \ldots, Z$ (which we can think of as, for instance $[Adam], [Betty], \ldots, [Zeek]$). Again, these are the same sets that we used to partition people into in Example 3.152.

In these examples, there seems to be a connection between the equivalence classes of the relation and the sets in a partition. As the next theorem illustrates, this is no coincidence.

Theorem 3.192. *Let $S \neq \varnothing$ be a set. Every equivalence relation on S induces a partition of S and vice-verse.*

Proof: *By Lemma 3.188, if R is an equivalence relation on S then*

$$S = \bigcup_{a \in S} [a],$$

and $[a] \cap [b] = \varnothing$ if a is not related to b. This proves the first half of the theorem.

Conversely, let

$$S = \bigcup_{\alpha} S_\alpha, \text{ where } S_\alpha \cap S_\beta = \varnothing \text{ if } \alpha \neq \beta,$$

be a partition of S. We define the relation R on S by letting aRb if and only if they belong to the same S_α. Since the S_α are mutually disjoint, it is clear that R is an equivalence relation on S and that for $a \in S_\alpha$, we have $[a] = S_\alpha$. □

Equivalence classes of an equivalence relation and partitions of sets are essentially the same thing. The main difference is in how we look at it. When thinking about equivalence relations/-classes, the focus is on what it means for two things to be related. When thinking about partitions, the focus is on what it means for an element to be in a particular subset of the partition.

Example 3.193. In light of Theorem 3.192, we can say that the relation defined by congruence modulo 4 partitions the set of integers into precisely 4 equivalence classes: [0], [1], [2], and [3]. That is, given any integer, it is contained in one (and only one) of these classes.

More generally, if $n > 2$, $\mathbb{Z}$ can be partitioned into n sets, $[0], [1], \ldots, [n-1]$, each of which is an equivalence class of the relation defined by congruence modulo n.

When we think about the partition, we are focused on the concept that each number x goes into one of the n subsets based on the value x mod n. On the other hand, when we think

about the relation of congruence modulo n, we are focused on the idea that x and y are in the same equivalence class iff $x \equiv y \pmod{n}$.

3.5 Reading Comprehension Questions

From Section 3.1.1

★**Question 3.1.** Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{2, 4, 6\}$. Which of the following notations makes sense? Explain what is wrong with the ones that do not make sense.
(a) $3 \subseteq A$. (b) $3 \in A$. (c) $\{3\} \in A$. (d) $\{3\} \subseteq A$. (e) $B \in A$. (f) $B \subseteq A$.

★**Question 3.2.** What is $|\{1, 2, 2, 3, 4, 5, 5\}|$?

★**Question 3.3.** Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6\}$, and C=$\{1,\ 3,\ 5,\ 7\}$.

(a) (i) Is $B \subseteq A$? (ii) Is $C \subseteq A$? (iii) Is $A \subseteq B$?

(b) Find $|A|$, $|B|$ and $|C|$.

(c) Are A, B, and C finite or infinite sets?

★**Question 3.4.** (a) Is $\mathbb{Z}^+ \subseteq \mathbb{Z}$? (b) Is $\mathbb{Z} \subseteq \mathbb{Z}^+$? (c) Is $\mathbb{Z} \subseteq \mathbb{Q}$? (d) Is $\mathbb{Q} \subseteq \mathbb{R}$? (e) Is $\mathbb{R} \subseteq \mathbb{Q}$?

★**Question 3.5.** Use a reasonable mathematical notation to express the set of perfect cubes (e.g. numbers like $8 = 2^3$ and $-27 = (-3)^3$).

★**Question 3.6.** Use a reasonable mathematical notation to express the set of all numbers that have at most 2 digits past the decimal point. For instance, the set contains 7, 3.4, and 45.98, but does not contain 867.5309. (Hint: There is a really easy way to express this if you give it a little bit of thought. On the other hand, do not overthink it or you will come up with something more complicated than necessary.)

★**Question 3.7.** Let A be a set. Is $A \in P(A)$? Is $A \subseteq P(A)$?

★**Question 3.8.** Let A be a set with $|A| = 5$. How many subsets does A have? (Hint: don't work too hard on this one!)

★**Question 3.9.** Let $A = \{a, b, c, d, e\}$.

(a) What are $|A|$ and $|P(A)|$?

(b) Is $\{\{a\}, \{b, c\}, \{a, c, e\}\} \subseteq A$? If not, explain why not.

(c) Is $\{b, c, e\} \subseteq A$? If not, explain why not.

(d) Is $\{b, c, e\} \in A$? If not, explain why not.

(e) Is $\{\{a\}, \{b, c\}, \{a, c, e\}\} \subseteq P(A)$? If not, explain why not.

(f) Is $\{b, c, e\} \subseteq P(A)$? If not, explain why not.

(g) Is $\{b, c, e\} \in P(A)$? If not, explain why not.

From Section 3.1.2

★**Question 3.10.** Let $U = \{a, b, c, d, \ldots, z\}$ (the letters in the English alphabet) be the universal set, $V = \{a, e, i, o, u\}$ (the vowels), $C = \overline{V}$ (the consonants), and $R = \{a, b, d, g, k, p, v\}$ (some random letters). Find each of the following: (a) $C \cup R$ (b) $C \cap R$ (c) $V \cap R$ (d) $R \setminus C$ (e) $\overline{C \cup R}$

★**Question 3.11.** True or False?

(a) $A \cap B \subseteq A$

(b) $A \cup B \subseteq A$

(c) $A \setminus B \subseteq B$

(d) The intersection of the complements of two sets is the same as the complement of the union of the two sets.

★**Question 3.12.** Let $A = \{1, 2, 3, 4\}$ and $B = \{u, v, w, x, y, z\}$.

(a) Give 3 examples of elements in $A \times B$.

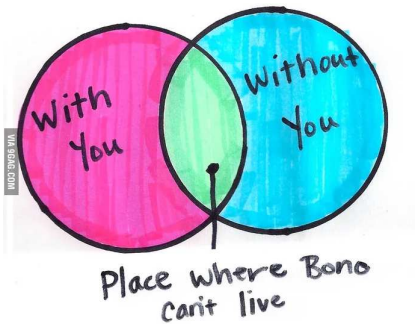
(b) Give 3 examples of elements in A^2.

(c) What is $|A \times B|$?

(d) What is $|A^3|$?

(e) What is $|P(A^2 \times B)|$?

★**Question 3.13.** The image to the right (which originated from https://9gag.com/gag/4169218) is a joke based on the *U2* song "With or without you," and in particular the lyric "I can't live with or without you" which is sung by the lead singer, Bono. What is wrong with the Venn diagram? Draw a correct Venn Diagram that expresses where Bono can't live.



From Section 3.1.3

★**Question 3.14.** Let A and B be sets.

(a) Let's say that I can prove that whenever $x \in A$, then $x \in B$. What did I just prove?

(b) Let's assume I have the proof from part (a), but I can also prove that whenever $x \in B$, then $x \in A$. Now what have I proven?

★**Question 3.15.** Give an informal proof of the second version of De Morgan's law (See Table 3.1) by describing the sets on both sides of the inequality and concluding that they are the same.

★**Question 3.16.** Use a set containment proof to prove the first complement law. That is, if A is a set and U is the universal set, prove that $A \cup \overline{A} = U$.

From Section 3.2

★**Question 3.17.** How can you use the mod operator to determine whether an integer is even or odd?

★**Question 3.18.** If you want to know what time it is 8 hours from now, can you use modular arithmetic to help you compute that? Explain. Does the answer change in any way if you are working with 24-hour military time versus 12-hour times with am/pm? Explain how the calculation can be done in both cases (using modular arithmetic, assuming it is appropriate).

★**Question 3.19.** Given integers a, b, and n, explain how you can determine whether or not $a \equiv b \pmod{n}$. Hint: There may be a helpful Theorem from this section.

★**Question 3.20.** Compute $\gcd(67890, 12345)$ using Euclid's algorithm.

★**Question 3.21.** Are 67890 and 12345 relatively prime? Explain.

★**Question 3.22.** Is the floor of the ceiling of a number always the same as the ceiling of the floor of a number? Explain, giving examples as necessary.

From Section 3.3.1

★**Question 3.23.** Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function defined by $f(x) = 2x$.

(a) What is the domain of f?

(b) What is the codomain of f?

(c) What is the range of f?

★**Question 3.24.** Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8\}$. Give an example of each of the following. If it is not possible, explain why.

(a) A function $f : A \to B$ that is one-to-one.

(b) A function $f : A \to B$ that is not one-to-one.

(c) A function $f : A \to B$ that is onto.

(d) A function $f : A \to B$ that is not onto.

(e) A function $f : A \to B$ that is bijective.

★**Question 3.25.** Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8, 10, 12\}$. Give an example of each of the following. If it is not possible, explain why.

(a) A function $f : A \to B$ that is one-to-one.

(b) A function $f : A \to B$ that is not one-to-one.

(c) A function $f : A \to B$ that is onto.

(d) A function $f : A \to B$ that is not onto.

(e) A function $f : A \to B$ that is bijective.

★**Question 3.26.** Let $f(x) = 2^x$ and $g(x) = x + 2$. Find $f \circ g$ and $g \circ f$.

From Section 3.3.2

★**Question 3.27.** Is each of the following true or false? If it is false, explain why.

(a) To show that f is one-to-one, you need to show that if $a = b$, then $f(a) = f(b)$.

(b) To show that f is *not* one-to-one, you only need to find two values in the domain that map to the same element of the codomain.

(c) To show that f is onto, you need to show that every element of the domain gets mapped to some element of the codomain.

(d) To show that f is onto, you can show that the range and codomain are exactly the same set.

(e) To show that f is *not* onto, you need to show that no elements of the range are mapped to.

(f) To show that f is invertible, you need to show that f is one-to-one and that f is onto.

★**Question 3.28.** Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3 - 8$. Prove that f is invertible and find its inverse.

From Section 3.4

★**Question 3.29.** Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $B = \{2, 4, 6, 8, 10\}$.

(a) Define a set C such that B, C is a partition of A.

(b) Define a set C such that B, C is a not partition of A because the sets are not disjoint.

(c) Define a set C such that B, C is a not partition of A because the union of the sets is not A.

(d) Define sets C and D such that B, C, D is a partition of A.

(e) Define sets C and D such that $B \cap D = C \cap D = \emptyset$, and $B \cup C \cup D = A$, but B, C, D, is a not partition of A.

★**Question 3.30.** Is $\{(1, 3), (456, 901), (867, 5309)\}$ a relation on $\mathbb{Z}$? Explain.

★**Question 3.31.** Define a partial order on the set of all human beings. Briefly explain why it is a partial order.

★**Question 3.32.** Define an equivalence relation on the set of all cars. Briefly explain why it is an equivalence relation. Then define a partition of the set of all cars that corresponds to the equivalence relation. Give a clear definition of each equivalence class (that is, each set in the partition), and if possible give a representative element from each subset.

★**Question 3.33.** Let B be the relation on $\mathbb{Z}^+$ such that $(x, y) \in B$ if x and y have the same number of 1s in their binary representation. For example, $3 = 11_2$ and $5 = 101_2$, so both 3 and 5 have two 1s in their binary representation. Thus, $(3, 5) \in B$ and $(5, 3) \in B$. On the other hand, $(3, 2) \notin B$ since $2 = 10_2$ has only one 1 in its binary representation.

(a) Is B an equivalence relation? Explain.

(b) Is B a partial order? Explain.

(c) Define a partition of $\mathbb{Z}^+$ based on the relation B. (Hint: The fact that I am asking this question should clue you in on the answer to one or more of the previous questions.) In other words, define sets $B_1, B_2, B_3 \ldots$ such that $\mathbb{Z}^+ = B_1 \cup B_2 \cup B_3 \cup \cdots$ and $B_i \cap B_j = \emptyset$ if $i \neq j$. To be clear, I am looking for a clear definition of B_i for a given value of i.

(d) Give the most obvious choice of a representative for each subset B_i. That is, choose an a_i such that $[a_i] = B_i$.

(e) Give at least 4 elements of B_2.

3.6 Problems

Problem 3.1. Draw a Venn diagram showing $A \cap (B \cup C)$, where A, B, and C are sets.

Problem 3.2. Assume A, B, and C are sets. Prove each of the following set identities using a set containment proof based on the basic definitions of $\cap$, $\cup$, etc. (see examples 3.61, 3.64, and 3.65).

(a) $(A \cap B \cap C) \subseteq (A \cap B)$.

(b) $A \cap B \subseteq A \cup B$.

(c) $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

(d) $(A - B) \setminus C \subseteq A \setminus C$.

Problem 3.3. Prove each of the following set identities using a set containment proof based on the basic definitions of $\cap$, $\cup$, etc. (see examples 3.61, 3.64, and 3.65).

(a) $A \cup (A \cap B) = A$.

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(c) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

(d) $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$. (This one is a little tricky.)

Problem 3.4. Rusty has 20 marbles of different colors: black, blue, green, and yellow. Seventeen of the marbles are not green, five are black, and 12 are not yellow. How many blue marbles does he have?

Problem 3.5. You need to settle an argument between your boss (who can fire you) and your professor (who can fail you). They are trying to decide who to invite to the Young Accountants Volleyball League. They want to invite freshmen who are studying accounting and are at least 6 feet tall. They have a list of all students.

(a) Your boss says they should make a list of all freshmen, a list of all accounting majors, and a list of everyone at least 6 feet tall. They should then combine the lists (removing duplicates) and invite those on the combined list. Is he correct? Explain. If he is not correct, describe in the simplest possible terms who ends up on his guest list.

(b) Your professor says they should make a list of everyone who is not a freshman, a list of everyone who does not do accounting, and a list of everyone who is under 6 feet tall. They should make a fourth list that contains everyone who is on all three of the prior lists. Finally, they should remove from the original list everyone on this fourth list, and invite the remaining students. Is he correct? Explain. If he is not correct, describe in the simplest possible terms who ends up on his guest list.

(c) Give a simple description of how the guest list should be created.

Problem 3.6. Using words, explain what $53 \bmod 7 = 4$ means.

Problem 3.7. Let a be a integer such $a \leq 17/3$. What can you say about a? Prove your claim.

Problem 3.8. Compute each of the following. If 2 answers are possible, give both.

(a) 23 mod 10
(b) $-14 \bmod 10$
(c) 8675309 mod 10
(d) 3 mod 5
(e) 34 mod 5
(f) $-8 \bmod 5$
(g) 13 mod 12
(h) 144 mod 12
(i) 7 mod 12
(j) $-7 \bmod 12$
(k) 3 mod 2
(l) $-3 \bmod 2$

Problem 3.9. Compute each of the following.

(a) $\lfloor 2.72 \rfloor$
(b) $\lceil 2.72 \rceil$
(c) $\lfloor 3.1415 \rfloor$
(d) $\lceil 3.1415 \rceil$
(e) $\lfloor \lceil 3.1415 \rceil \rfloor$
(f) $\lceil \lfloor 3.1415 \rfloor \rceil$
(g) $\lfloor 3/2 \rfloor$
(h) $\lfloor 5/4 \rfloor$
(i) $\lfloor 8.675309 \rfloor \bmod 3$
(j) $\lceil 8.675309 \rceil \bmod 3$

Problem 3.10. Prove or disprove: If a is a real number and n is an integer, then $\lfloor a \rfloor \bmod n = \lfloor a \bmod n \rfloor$.

Problem 3.11. Recall that $a \equiv b \pmod{n}$ iff $a - b = kn$ for some integer k. Use this definition of congruence modulo n to prove Theorem 3.90. (Note: This is an if and only if proof, so you need to prove both ways.)

Problem 3.12. Let $a, b \in \mathbb{R}$, $a \neq 0$, and define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$. Prove that f is one-to-one and onto.

Problem 3.13. Let a and b be real numbers with $a \neq 0$. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = a\,x + b$. Show that f is invertible. Then find f^{-1}.

Problem 3.14. Prove or disprove: if a, b, and c are real numbers with $a \neq 0$, then the function $f(x) = a\,x^2 + b\,x + c$ is invertible.

Problem 3.15. Prove that if f and g are onto, then $f \circ g$ is also onto.

Problem 3.16. Let $f(x) = x + \lfloor x \rfloor$ be a function on $\mathbb{R}$. (This one is a little tricky.)

(a) Prove or disprove that f is one-to-one.

(b) Prove or disprove that f is onto.

(c) Prove or disprove that f is invertible.

Problem 3.17. Find the inverse of the function $f(x) = x^3 + 1$ over the real numbers.

Problem 3.18. Let f be the function on $\mathbb{Z}^+$ that maps x to the number of bits required to represent x in binary. For instance, $f(1) = 1$, $f(2) = 2$, $f(3) = 2$, $f(4) = 3$, $f(10) = 4$, etc. Hint: The number 2^n requires $n + 1$ bits to represent (a single 1 followed by n zeros). You may be able to use this fact in one of your proofs.

(a) Prove or disprove that f is one-to-one.

(b) Prove or disprove that f is onto.

(c) Prove or disprove that f is invertible.

Problem 3.19.

Consider the relation $R = \{(1,2),(1,3),(3,5),(2,2),(5,5),(5,3),(2,1),(3,1)\}$ on set $\{1,2,3,4,5\}$. Is R reflexive? symmetric? anti-symmetric? transitive? an equivalence relation? a partial order?

Problem 3.20. Let X be the set of all people. Which of the following are equivalence relations? Prove it.

(a) $R_1 = \{(a,b) \in X^2 | a \text{ and } b \text{ are the same height}\}$

(b) $R_2 = \{(a,b) \in X^2 | a \text{ is taller than } b\}$

(c) $R_3 = \{(a,b) \in X^2 | a \text{ is at least as tall as } b\}$

(d) $R_4 = \{(a,b) \in X^2 | a \text{ and } b \text{ have the same last name}\}$

(e) $R_5 = \{(a,b) \in X^2 | a \text{ has the same kind of pet as } b\}$

Problem 3.21. Repeat the previous problem, but which are partial orders? Prove it.

Problem 3.22. Define three different equivalence relations on the set of all TV shows. For each, give examples of the equivalence classes, including one representative from each. Prove that each is an equivalence relation.

Problem 3.23. Define a relation on the set of all Movies that is *not* an equivalence relation.

Problem 3.24. Let $A = \{1,2,\ldots,n\}$. Let R be the relation on $P(A)$ (the power set of A) such that $a, b \in P(A)$ are related iff $|a| = |b|$. Prove that R is an equivalence relation. What are the equivalence classes of R?

Chapter 4: Sequences, Summations, and Matrices

4.1 Sequences

Definition 4.1. *A* **sequence** *of real numbers is a function whose domain is the set of natural numbers and whose output is a subset of the real numbers. We usually denote a sequence by one of the notations*

$$a_0, a_1, a_2, \ldots$$

or

$$\{a_n\}_{n=0}^{+\infty}$$

or

$$\{a_n\}.$$

The last notation is just a shorthand for the second notation.

Note: *Since sequences are functions, sometimes function notation is used. That is, $a(n)$ instead of a_n.*

We will be mostly interested in two types of sequences. The first type are sequences that have an explicit formula for their n-th term. They are said to be in *closed form*.

Example 4.2. Let $a_n = 1 - \frac{1}{2^n}, n = 0, 1, \ldots$. Then $\{a_n\}_{n=0}^{+\infty}$ is a sequence for which we have an explicit formula for the n-th term. The first five terms are

$$\begin{aligned}
a_0 &= 1 - \tfrac{1}{2^0} = 1 - 1 = 0,\\
a_1 &= 1 - \tfrac{1}{2^1} = 1 - \tfrac{1}{2} = \tfrac{1}{2},\\
a_2 &= 1 - \tfrac{1}{2^2} = 1 - \tfrac{1}{4} = \tfrac{3}{4},\\
a_3 &= 1 - \tfrac{1}{2^3} = 1 - \tfrac{1}{8} = \tfrac{7}{8},\\
a_4 &= 1 - \tfrac{1}{2^4} = 1 - \tfrac{1}{16} = \tfrac{15}{16}.
\end{aligned}$$

Note: *Sometimes we may not start at $n = 0$. In that case we may write*

$$a_m, a_{m+1}, a_{m+2}, \ldots,$$

or

$$\{a_n\}_{n=m}^{+\infty},$$

where m is a non-negative integer. Most sequences we will deal with will start with $m = 0$ or $m = 1$.

★**Exercise 4.3.** Let $\{x_n\}$ be the sequence defined by $x_n = 1 + (-2)^n, n = 0, 1, 2, \ldots$. Find the first five terms of $\{x_n\}$.

(a) $x_0 =$ _____

(b) $x_1 =$ _____

(c) $x_2 =$ _____

(d) $x_3 =$ _____

(e) $x_4 =$ _____

★**Exercise 4.4.** Find the first five terms of the following sequences.

(a) $x_n = 1 + \left(-\frac{1}{2}\right)^n, n = 0, 1, 2, \ldots$

$x_0 =$ _____ $x_1 =$ _____ $x_2 =$ _____

$x_3 =$ _____ $x_4 =$ _____

(b) $x_n = n! + 1, n = 0, 1, 2, \ldots$

$x_0 =$ _____ $x_1 =$ _____ $x_2 =$ _____

$x_3 =$ _____ $x_4 =$ _____

(c) $x_n = \dfrac{1}{n! + (-1)^n}, n = 2, 3, 4, \ldots$

$x_2 =$ _____ $x_3 =$ _____ $x_4 =$ _____

$x_5 =$ _____ $x_6 =$ _____

(d) $x_n = \left(1 + \frac{1}{n}\right)^n, n = 1, 2, \ldots$

$x_1 =$ _____ $x_2 =$ _____ $x_3 =$ _____

$x_4 =$ _____ $x_5 =$ _____

The second type of sequence are defined using *recurrence relations*.

Definition 4.5. *A* **recurrence relation** *is an equation that defines each term of a sequence based on one or more previous terms of the sequence. More specifically, a recurrence relation for a sequence* $\{a_n\}$ *will define* a_n *based on (some of) the values of* a_0, a_1, $\ldots$, a_{n-1}.

Example 4.6. Let $x_0 = 1$, $x_n = \left(1 + \frac{1}{n}\right) x_{n-1}$, for $n = 1, 2, \ldots$. Then $\{x_n\}_{n=0}^{+\infty}$ is a recursively defined sequence. The terms $x_1, x_2, \ldots, x_5$ are

$$\begin{aligned}
x_1 &= \left(1+\tfrac{1}{1}\right) x_0 = \left(1+\tfrac{1}{1}\right) 1 = 1+1 = 2.\\
x_2 &= \left(1+\tfrac{1}{2}\right) x_1 = \left(1+\tfrac{1}{2}\right) 2 = 2+1 = 3.\\
x_3 &= \left(1+\tfrac{1}{3}\right) x_2 = \left(1+\tfrac{1}{3}\right) 3 = 3+1 = 4.\\
x_4 &= \left(1+\tfrac{1}{4}\right) x_3 = \left(1+\tfrac{1}{4}\right) 4 = 4+1 = 5.\\
x_5 &= \left(1+\tfrac{1}{5}\right) x_4 = \left(1+\tfrac{1}{5}\right) 5 = 5+1 = 6.
\end{aligned}$$

Notice that in the previous example, we gave an explicit definition of x_0. This is called an *initial condition*. In order to specify a sequence, a recurrence relation needs one or more initial conditions. Without them, we have an abstract definition of a sequence, but cannot compute any values since there is no "starting point." Also note that different initial conditions can be specified for the same recurrence relation, resulting in different sequences being generated.

When we find an explicit formula (or *closed formula*) for a recurrence relation, we say we have *solved* the recurrence relation.

Example 4.7. Given the values we computed in Example 4.6, it seems relatively clear that $x_n = n + 1$ is a solution for that recurrence relation.

Note: *It is important to be careful about jumping to conclusions too quickly when solving recurrence relations.*[a] *Although it turns out that in the previous example,* $x_n = n + 1$ *is the correct closed form (we will prove it shortly), just because it works for the first 5 terms does not necessarily imply that the pattern continues.*

[a] These comments also apply to other problems that involve seeing a pattern and finding an explicit formula.

★**Exercise 4.8.** Let $\{x_n\}$ be the sequence defined by

$$x_0 = 1, x_n = 5 \cdot x_{n-1}, \text{ for } n = 1, 2, \ldots.$$

Find a closed form for x_n. (Hint: Start by computing x_1, x_2, x_3, etc. until you see the pattern.)

★**Exercise 4.9.** Let $\{x_n\}$ be the sequence defined by

$$x_0 = 1, x_n = n \cdot x_{n-1}, \text{ for } n = 1, 2, \ldots.$$

Find a closed form for x_n.

★**Evaluate 4.10.** Define $\{a_n\}$ by $a(0) = 1$, $a(1) = 2$, and

$$a_n = \left\lfloor \frac{1+\sqrt{5}}{2} \times a_{n-1} \right\rfloor + a_{n-2}$$

for $n \geq 2$. Find a closed form for a_n.

Solution: We can see that

$$\begin{aligned} a_2 &= \left\lfloor \tfrac{1+\sqrt{5}}{2} \times a_1 \right\rfloor + a_0 = \left\lfloor \tfrac{1+\sqrt{5}}{2} \times 2 \right\rfloor + 1 = 4 \\ a_3 &= \left\lfloor \tfrac{1+\sqrt{5}}{2} \times a_2 \right\rfloor + a_1 = \left\lfloor \tfrac{1+\sqrt{5}}{2} \times 4 \right\rfloor + 2 = 8 \\ a_4 &= \left\lfloor \tfrac{1+\sqrt{5}}{2} \times a_3 \right\rfloor + a_2 = \left\lfloor \tfrac{1+\sqrt{5}}{2} \times 8 \right\rfloor + 4 = 16 \end{aligned}$$

(You can verify these with a calculator). At this point it seems relatively clear that $a_n = 2^n$.

Evaluation _____

_____

Did you catch what happened in the previous Evaluate exercise? The 'obvious' solution wasn't correct. If you missed this, go back and read the solution.

Generally speaking, you need to *prove* that the closed form is correct. One way to do this is to plug it back into the recursive definition. If we can plug it into the right hand side of the recursive definition and are able to simplify it to the left hand side, then it must be a solution. We also have to verify that it works for the initial condition(s).

As an analogy, how do you know that $x = -1$ is a solution to the equation $x^2 + 2x + 1 = 0$? You plug it in to get $(-1)^2 + 2(-1) + 1 = 1 - 2 + 1 = 0$. Since we got 0, $x = -1$ is a solution. We do something similar for recurrence relations, except that what we are plugging in is a formula instead of just a number.

Example 4.11. Prove that $x_n = n + 1$ is a solution to the recurrence relation given by

$$x_0 = 1, \quad x_n = \left(1 + \frac{1}{n}\right) x_{n-1}, \quad n = 1, 2, \ldots.$$

Proof: To prove that $x_n = n + 1$ is a solution for $n \geq 0$, we need to show two things. First, that it works for the initial condition. Since $x_0 = 1 = 0 + 1$, it works for the initial condition. Second, that if we plug it into the right hand side of the recursive definition, that we can simplify it to x_n. Doing so, we get

$$\begin{aligned} \left(1 + \frac{1}{n}\right) x_{n-1} &= \left(1 + \frac{1}{n}\right) ((n-1) + 1) \\ &= \left(\frac{n+1}{n}\right) n \\ &= n + 1 \\ &= x_n \end{aligned}$$

Since plugging the solution back in verifies the recurrence relation, $x_n = n + 1$ is a solution to the recurrence relation.

If you are confused by the first step of algebra, remember that we are assuming that $x_n = n + 1$ for $n \geq 0$. Thus, $x_{n-1} = (n-1) + 1 = n$, since we are just plugging in $n - 1$ instead of n. □

★**Exercise 4.12.** Prove that your solution to Exercise 4.8 is correct.

★**Exercise 4.13.** Prove that your solution to Exercise 4.9 is correct.

★**Evaluate 4.14.** Determine what `ferzle(n)` (below) returns for $n = 0, 1, 2, 3, 4$ and then re-write `ferzle` without using recursion, making it as efficient as possible.[a]

```
int ferzle(int n) {
    if(n<=0) {
        return 3;
    } else {
        return ferzle(n-1) + 2;
    }
}
```

Solution: First, we can see that ferzle(0) returns 3 since it executes the code in the if statement. ferzle(1) returns ferzle(0)+2, which is $3+2=5$. ferzle(2) returns ferzle(1)+2, which is $5+2=7$. ferzle(3) returns ferzle(2)+2, which is $7+2=9$. ferzle(4) returns ferzle(3)+2, which is $9+2=11$. Notice that $11 = 2*4+3$, $9 = 2*3+3$, $7 = 2*2+3$, $5 = 2*1+3$, and $3 = 2*0+3$. From this, it is pretty clear that ferzle(n) returns $2n+3$. Thus, my simplified function is as follows:

```
int ferzle(int n) {
    return 2*n+3;
}
```

Evaluation _____

[a] Although we have not formally covered recursion yet, we expect that you have seen it before and know enough to follow this example. If not, ask your instructor or a friend for help.

★**Exercise 4.15.** Fix the code from the solution given in Evaluate 4.14 so that it still uses the closed form, but works correctly for all values of n.

```
int ferzle(int n) {




}
```

A more complete discussion of solving recurrences appears in Chapter 5.

The following is a famous example of a recursively defined sequence that we will revisit several times.

Example 4.16. The *Fibonacci sequence* is a sequence of numbers that is of interest in various mathematical and computing applications. They are defined using the following recurrence relation:[a]

$$f_n = \begin{cases} 0 & \text{if } n{=}0 \\ 1 & \text{if } n{=}1 \\ f_{n-1} + f_{n-2} & \text{if } n > 1 \end{cases}$$

In words, each Fibonacci number (beyond the first two) is the sum of the previous two. The first few are $f_0 = 0$, $f_1 = 1$,

$$\begin{aligned} f_2 &= f_1 + f_0 = 1 + 0 = 1, \\ f_3 &= f_2 + f_1 = 1 + 1 = 2, \\ f_4 &= f_3 + f_2 = 2 + 1 = 3, \\ f_5 &= f_4 + f_3 = 3 + 2 = 5, \\ f_6 &= f_5 + f_4 = 5 + 3 = 8, \\ f_7 &= f_6 + f_5 = 8 + 5 = 13. \end{aligned}$$

Later we will see the closed form for the Fibonacci sequence. If you are really adventurous, you might consider trying to determine it yourself. But be warned: It is not a simple formula that you will come up with by just looking at some of the Fibonacci numbers.

[a] In the remainder of the book, when you see f_k, you should assume it refers to the k-th Fibonacci number unless otherwise specified.

Definition 4.17. *A sequence* $\{a_n\}_{n=0}^{+\infty}$ *is said to be*

- **increasing** *if* $a_n \leq a_{n+1}\ \forall n \in \mathbb{N}$
- **strictly increasing** *if* $a_n < a_{n+1}\ \forall n \in \mathbb{N}$
- **decreasing** *if* $a_n \geq a_{n+1}\ \forall n \in \mathbb{N}$
- **strictly decreasing** *if* $a_n > a_{n+1}\ \forall n \in \mathbb{N}$

Some people call these sequences **non-decreasing**, **increasing**, **non-increasing**, *and* **decreasing**, *respectively.*

A sequence is called **monotonic** *if it is any of these, and* **non-monotonic** *if it is none of these.*

Example 4.18. Recall that $0! = 1$, $1! = 1$, $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$, etc. Prove that the sequence $x_n = n!, n = 0, 1, 2, \ldots$ is strictly increasing for $n \geq 1$.

Proof: For $n > 1$ we have

$$x_n = n! = n(n-1)! = nx_{n-1} > x_{n-1},$$

since $n > 1$. This proves that the sequence is strictly increasing. □

★**Question 4.19.** Notice in this first example we concluded that the sequence is strictly increasing since we showed that $x_n > x_{n-1}$. But according to the definition we need to show that $x_n < x_{n+1}$. So did we do something wrong? Explain.

Answer _____

_____

_____

Example 4.20. Prove that the sequence $x_n = 2 + \frac{1}{2^n}$, $n = 0, 1, 2, \ldots$ is strictly decreasing.

Proof: We have

$$\begin{aligned} x_{n+1} - x_n &= \left(2 + \frac{1}{2^{n+1}}\right) - \left(2 + \frac{1}{2^n}\right) \\ &= \frac{1}{2^{n+1}} - \frac{1}{2^n} \\ &= -\frac{1}{2^{n+1}} \\ &< 0. \end{aligned}$$

Thus, $x_{n+1} - x_n < 0$, so $x_n > x_n{+}1$, i.e., the sequence is strictly decreasing. □

★**Exercise 4.21.** Prove that the sequence $x_n = \frac{n^2+1}{n}$, $n = 1, 2, \ldots$ is strictly increasing.

★**Exercise 4.22.** Decide whether the following sequences are increasing, strictly increasing, decreasing, strictly decreasing, or non-monotonic. You do not need to prove your answer, but give a brief justification.

(a) $x_n = n$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(b) $x_n = (-1)^n n$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(c) $x_n = \dfrac{1}{n!}$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(d) $x_n = \dfrac{n}{n+1}$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(e) $x_n = n^2 - n$, $n = 1, 2, \ldots$

Answer _____

_____

(f) $x_n = n^2 - n$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(g) $x_n = (-1)^n$, $n = 0, 1, 2, \ldots$

Answer _____

_____

(h) $x_n = 1 - \dfrac{1}{2^n}$, $n = 0, 1, 2, \ldots$

Answer _____

(i) $x_n = 1 + \dfrac{1}{2^n}$, $n = 0, 1, 2, \ldots$

Answer _____

There are two types of sequences that come up often. We will briefly discuss each.

Definition 4.23. *A* **geometric progression** *is a sequence of the form*

$$a,\ ar, ar^2,\ ar^3,\ ar^4, \ldots,$$

where a (the **initial term***) and r (the* **common ratio***) are real numbers. That is, a geometric progression is a sequence in which every term is produced from the preceding one by multiplying it by a fixed number.*

Notice that the first term can be written as ar^0, so like an array in many programming languages, the terms of a geometric progression are indexed starting at 0. Thus, the n-th term is ar^{n-1}. If $a = 0$ then every term is 0. If $ar \neq 0$, we can find r by dividing any term by the previous term.

Example 4.24. Find the 11-th term of the geometric progression

$$3, 6, 12, 24, \ldots.$$

Solution: Since this is a geometric progression, $a = 3$ since the first term is always a. To determine r, we need to find the ratio between any two terms. For instance, $24/12 = 2$ or $12/6 = 2$. So $r = 2$ in this case. Thus, the sequence is $\{3 \cdot 2^k\}$, and the 11-th term is $3 \cdot 2^{10} = 3 * 1024 = 3072$.

Example 4.25. Find the 35-th term of the geometric progression

$$\frac{1}{\sqrt{2}},\ -2,\ \frac{8}{\sqrt{2}}, \ldots.$$

Solution: $a = \frac{1}{\sqrt{2}}$, and the common ratio is $r = -2/\frac{1}{\sqrt{2}} = -2\sqrt{2}$. Thus, the n-th term is $\frac{1}{\sqrt{2}}\left(-2\sqrt{2}\right)^{n-1}$. Hence the 35-th term is $\frac{1}{\sqrt{2}}\left(-2\sqrt{2}\right)^{34} = \frac{2^{51}}{\sqrt{2}} = 1125899906842624\sqrt{2}$.

★**Exercise 4.26.** Find the 17-th term of the geometric progression

$$-\frac{2}{3^{17}},\ \frac{2}{3^{16}},\ -\frac{2}{3^{15}},\dots .$$

Example 4.27. The fourth term of a geometric progression is 24 and its seventh term is 192. Find its second term.

Solution: We are given that $ar^3 = 24$ and $ar^6 = 192$, for some a and r. Clearly, $ar \neq 0$, and so we find

$$\frac{ar^6}{ar^3} = r^3 = \frac{192}{24} = 8.$$

Thus, $r = 2$. Now, $a(2)^3 = 24$, giving $a = 3$. The second term is thus $ar = 6$.

★**Exercise 4.28.** The 6-th term of a geometric progression is 20 and the 10-th is 320. Find the absolute value of its third term.

Definition 4.29. *An* **arithmetic progression** *is a sequence of the form*

$$a,\ a+d, a+2d,\ a+3d,\ a+4d, \dots ,$$

where a (the **initial term***) and d (the* **common difference***) are real numbers. That is, an arithmetic progression is a sequence in which every term is produced from the preceding one by adding a fixed number.*

Example 4.30. If $s_n = 3n - 7$, then $\{s_n\}$ is an arithmetic progression with $a = -7$ and $d = 3$ (assuming we begin with s_0).

Note: *Notice that geometric progressions are essentially a discrete version of an exponential function and arithmetic progressions are a discrete version of a linear function. One consequence of this is that a sequence cannot be both of these unless it is the sequence $a, a, a, \ldots$ for some a.*

Example 4.31. Consider the sequence

$$4, 7, 10, 13, 16, 19, 22, \ldots .$$

Assuming the pattern continues, is this a geometric progression? Is it an arithmetic progression?

Solution: It is easy to see that each term is 3 more than the previous term. Thus, this is an arithmetic progression with $a = 4$ and $d = 3$. Clearly it is therefore not geometric.

★**Question 4.32.** Tests like the SAT and ACT often have questions such as the following.

23. Given the sequence of numbers 2, 9, 16, 23, what will the 8th term of the sequence be? (a) 60 (b) 58 (c) 49 (d) 51 (e) 56

(a) What is the 'correct' answer to this question?

Answer _____

_____

(b) Why did I put 'correct' in quotes in the previous question?

Answer _____

_____

Now let's see if you can correctly identify geometric and/or arithmetic sequences.

★**Question 4.33.** Determine whether or not the following sequences are geometric and/or arithmetic. Explain your answer.

(a) The sequence from Example 4.8.

Answer _____

(b) The sequence from Example 4.9.

Answer _____

(c) The sequence generated by `ferzle(n)` in Evaluate 4.14 on the non-negative inputs.

Answer _____

4.2 Sums and Products

When there is a need to add or multiply terms from a sequence, *summation notation* (or *sum notation*) and *product notation* come in handy. We first introduce sum notation.

Definition 4.34. *Let $\{a_n\}$ be a sequence. Then for $1 \leq m \leq n$, where m and n are integers, we define*

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \cdots + a_n.$$

We call k the **index of summation** *and m and n the* **limits** *of the summation. More specifically, m is the* **lower limit** *and n is the* **upper limit**. *Each a_k is a* **term** *of the sum.*

Note: *We often use i, j, and k as index variables for sums, although any letters can be used.*

Example 4.35. We can express the sum $1 + 3 + 3^2 + 3^3 + \cdots + 3^{49}$ as

$$\sum_{i=0}^{49} 3^i.$$

(Recall that $3^0 = 1$, so the first term fits the pattern.)

★**Exercise 4.36.** Write $1 + y + y^2 + y^3 + \cdots + y^{100}$ using sum notation.

Example 4.37. Write the following sum using sum notation.

$$1 - y + y^2 - y^3 + y^4 - y^5 + \cdots - y^{99} + y^{100}$$

Solution: This is a lot like the previous exercise, except that every other term is negative. So how do we get those terms to be negative? The standard trick relies on the fact that $(-1)^i$ is 1 if i is even and -1 if i is odd. Thus, we can multiple each term by $(-1)^i$ for an appropriate choice of i. Since the odd powers are the negative ones, this is easy:

$$\sum_{i=0}^{100} (-1)^i y^i \qquad \text{or} \qquad \sum_{i=0}^{100} (-y)^i$$

Note: *You might be tempted to give the following solution to the previous problem:*

$$\sum_{i=0}^{100} -y^i.$$

As we will see shortly, this is the same as

$$-\sum_{i=0}^{100} y^i,$$

which is not the correct answer. The bottom line: Always use parentheses in the appropriate locations, especially when negative numbers are involved!

★**Exercise 4.38.** Write $1 + y^2 + y^4 + y^6 + \cdots + y^{100}$ using sum notation.

Note: *If you struggled understanding the two solutions to the previous example, it might be time to review the basic algebra rules involving exponents. We will just give a few of them here. You can find more extensive lists in an algebra book or various reputable online sources. We have already used the fact that if $x \neq 0$, then $x^0 = 1$. In addition, if $x, a, b \in \mathbb{R}$ with $x > 0$, then*

$$(x^a)^b = x^{ab}, \qquad x^a x^b = x^{a+b}, \qquad (x^{-a}) = \frac{1}{x^a}, \qquad \text{and} \qquad x^{\frac{a}{b}} = \sqrt[b]{x^a} = \left(\sqrt[b]{x}\right)^a.$$

As with sequences, we are often interested in obtaining *closed forms* for sums. We will present several important formulas, along with a few techniques to find closed forms for sums.

Example 4.39. It should not be too difficult to see that

$$\sum_{k=1}^{20} 1 = 20$$

since this sum is adding 20 terms, each of which is 1. But notice that

$$\sum_{k=0}^{19} 1 = \sum_{k=200}^{219} 1 = 20$$

since both of these sums are also adding 20 terms, each of which is 1. In other words, if the variable of summation (the k) does not appear in the sum, then the only thing that matters is how many terms the sum involves.

★**Exercise 4.40.** Find each of the following.

(a) $\sum_{k=5}^{6} 1 =$ _____

(b) $\sum_{k=20}^{30} 1 =$ _____

(c) $\sum_{k=1}^{100} 1 =$ _____

(d) $\sum_{k=0}^{100} 1 =$ _____

Hopefully you noticed that the previous example and exercise can be generalized as follows.

Theorem 4.41. *If $a, b \in \mathbb{Z}$, then*

$$\sum_{k=a}^{b} 1 = (b - a + 1).$$

Proof: *This sum has $b - a + 1$ terms since there are that many number between a and b, inclusive. Since each of the terms is 1, the sum is obviously $b - a + 1$.* □

Example 4.42. If we apply the previous theorem to the sums in Example 4.39, we would obtain $20 - 1 + 1 = 20$, $19 - 0 + 1 = 20$, and $219 - 200 + 1 = 20$.

Next is a simple theorem based on the distributive law that you learned in grade school.

Theorem 4.43. *If $\{x_n\}$ is a sequence and a is a real number, then*

$$\sum_{k=m}^{n} a \cdot x_k = a \sum_{k=m}^{n} x_k.$$

Example 4.44. Using Theorems 4.41 and 4.43, we can see that

$$\sum_{k=5}^{17} 4 = 4 \sum_{k=5}^{17} 1 = 4 \cdot (17 - 5 + 1) = 4 \cdot 13 = 52.$$

★**Exercise 4.45.** Find each of the following.

(a) $\sum_{k=5}^{6} 5 =$ _____

(b) $\sum_{k=20}^{30} 200 =$ _____

We can combine Theorems 4.41 and 4.43 to obtain the following.

Theorem 4.46. *If $a, b \in \mathbb{Z}$ and $c \in \mathbb{R}$, then*

$$\sum_{k=a}^{b} c = (b - a + 1)c.$$

Proof: *Using Theorem 4.43, we have*

$$\sum_{k=a}^{b} c = c \sum_{k=a}^{b} 1 = (b - a + 1)c.$$

□

Example 4.47. We can compute the sum from Example 4.44 by using Theorem 4.46 to obtain

$$\sum_{k=5}^{17} 4 = (17 - 5 + 1)4 = 52.$$

Both ways of computing this sum are valid, so feel free to use whichever you prefer.

★**Exercise 4.48.** Find each of the following.

(a) $\sum_{k=20}^{30} 200 =$ _____

(b) $\sum_{k=1}^{100} 9 =$ _____

(c) $\sum_{k=0}^{100} 9 =$ _____

★**Evaluate 4.49.** Compute $\sum_{k=25}^{75} 10$.

Solution: This is just $10(75-25) = 10 * 50 = 500$.

Evaluation _____

_____

The following sum comes up often and should be committed to memory. The proof involves a nice technique that adds the terms in the sum twice, in a different order, and then divides the result by two. This is known as Gauss' trick.

Theorem 4.50. *If n is a positive integer, then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Proof: *Let $S = \sum_{k=1}^{n} k$ for shorthand. Then we can see that*

$$S = 1 + 2 + 3 + \cdots + n$$

and by reordering the terms,

$$S = n + (n-1) + \cdots + 1.$$

Adding these two quantities,

$$\begin{array}{rcccccccc} S & = & 1 & + & 2 & + & \cdots & + & n \\ S & = & n & + & (n-1) & + & \cdots & + & 1 \\ \hline 2S & = & (n+1) & + & (n+1) & + & \cdots & + & (n+1) \\ & = & n(n+1), & & & & & & \end{array}$$

since there are n terms. Dividing by 2, we obtain $S = \frac{n(n+1)}{2}$, as was to be proved. □

Example 4.51.

$$\sum_{k=1}^{10} k = \frac{10(10+1)}{2} = \frac{10 \cdot 11}{2} = 55.$$

★**Exercise 4.52.** Compute each of the following.

(a) $\sum_{k=1}^{20} k =$ _____

(b) $\sum_{k=1}^{100} k =$ _____

(c) $\sum_{k=1}^{1000} k =$ _____

★**Evaluate 4.53.** Compute $\sum_{k=1}^{30} k$.

Solution 1: $\sum_{k=1}^{30} k = 29 * 30/2 = 435.$

Evaluation _____

_____

Solution 2: $\sum_{k=1}^{30} k = k \sum_{k=1}^{30} 1 = k(30 - 1 + 1) = 30k.$

Evaluation _____

_____

Note: *A common error is to think that the sum of the first n integers is $n(n-1)/2$ instead of $n(n+1)/2$. Whenever I use the formula, I double check my memory by computing $1+2+3$. In this case, $n = 3$. So is the correct answer $3 \cdot 2/2 = 3$ or $3 \cdot 4/2 = 6$? Clearly it is the latter. Then I know that the correct formula is $n(n+1)/2$. You can use any positive value of n to check the formula. I use 3 out of habit.*

★**Question 4.54.** Is it true that $\sum_{k=0}^{n} k = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$? Explain.

Answer _____

Theorem 4.55. *If $\{x_k\}$ and $\{y_k\}$ are sequences, then for any $n \in \mathbb{Z}^+$,*

$$\sum_{i=1}^{n} x_i + y_i = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i.$$

Proof: *This follows from the commutative property of addition.* □

Example 4.56.

$$\sum_{i=1}^{20} i + 5 = \sum_{i=1}^{20} i + \sum_{i=1}^{20} 5 = \frac{20 \cdot 21}{2} + 5 \cdot 20 = 210 + 100 = 310.$$

★**Exercise 4.57.** Compute the following sum

$\sum_{i=1}^{100} 2 - i =$ _____.

★**Exercise 4.58.** Prove that the sum of the first n odd integers is n^2.

The following example contains something called a *telescoping series*. It demonstrates that evaluating a telescoping series is fairly simple.

Example 4.59. Let $\{a_k\}$ be a sequence of real numbers. Show that $\sum_{i=1}^{n}(a_i - a_{i-1}) = a_n - a_0$.

Proof: We can see that

$$\begin{aligned}
\sum_{i=1}^{n}(a_i - a_{i-1}) &= \left(\sum_{i=1}^{n} a_i\right) - \left(\sum_{i=1}^{n} a_{i-1}\right) \\
&= (a_1 + a_2 + \cdots + a_{n-1} + a_n) - (a_0 + a_1 + a_2 + \cdots + a_{n-1}) \\
&= a_1 + a_2 + \cdots + a_{n-1} + a_n - a_0 - a_1 - a_2 - \cdots - a_{n-1} \\
&= (a_1 - a_1) + (a_2 - a_2) + \cdots + (a_{n-1} - a_{n-1}) + a_n - a_0 \\
&= a_n - a_0. \square
\end{aligned}$$

Example 4.60. Given what we know so far, how can we compute the following:

$$\sum_{k=50}^{100} k = ?$$

It turns out that this is not that hard. Notice that it is *almost* a sum we know. We know how to compute $\sum_{k=1}^{100} k$, but that has too many terms. Can we just subtract those terms to get the answer? What terms don't we want? Well, we don't want terms 1 through 49. But that is just $\sum_{k=1}^{49} k$. In other words,

$$\begin{aligned}\sum_{k=50}^{100} k &= \sum_{k=1}^{100} k - \sum_{k=1}^{49} k \\ &= \frac{100 \cdot 101}{2} - \frac{49 \cdot 50}{2} \\ &= 5050 - 1225 = 3825\end{aligned}$$

★**Exercise 4.61.** Compute each of the following.

(a) $\sum_{k=10}^{20} k =$ _____

(b) $\sum_{k=21}^{40} k =$ _____

★**Evaluate 4.62.** Compute the following.

$$\sum_{k=30}^{100} k.$$

Solution I:

$$\sum_{k=30}^{100} k = \sum_{k=1}^{100} k - \sum_{k=1}^{30} k = 100 \cdot 101/2 - 30 \cdot 31/2 = 5050 - 465 = 4585$$

Evaluation _____

_____

Solution 2:

$$\sum_{k=30}^{100} k = \sum_{k=1}^{100} k - \sum_{k=1}^{30} k = 99 \cdot 100/2 - 29 \cdot 30/2 = 4950 - 435 = 4515$$

Evaluation _____

_____

Solution 3:

$$\sum_{k=30}^{100} k = \sum_{k=1}^{100} k - \sum_{k=1}^{29} k = 100 \cdot 101/2 - 29 \cdot 30/2 = 5050 - 435 = 4615$$

Evaluation _____

_____

★**Question 4.63.** Explain why the following computation is incorrect. Then explain why the answer is correct even with the error(s).

$$\sum_{k=30}^{100} k = \sum_{k=1}^{100} k - \sum_{k=1}^{30} k = 100 \cdot 101/2 - 29 \cdot 30/2 = 5050 - 435 = 4615$$

Answer _____

_____

_____

_____

Theorem 4.64. *Let $n \in \mathbb{Z}^+$. Then the following hold.*

$$\begin{aligned}
\sum_{k=1}^{n} k^2 &= \frac{n(n+1)(2n+1)}{6} \\
\sum_{k=1}^{n} k^3 &= \frac{n^2(n+1)^2}{4} \\
\sum_{k=2}^{n} \frac{1}{(k-1)k} &= \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{(n-1)\cdot n} = \frac{n-1}{n}
\end{aligned}$$

We will prove Theorem 4.64 in the chapter on mathematical induction since that is perhaps the easiest way to prove these results. It is probably a good idea to attempt to commit the first two of these sums to memory since they come up on occasion.

★**Question 4.65.** Why does the third formula from Theorem 4.64 have a lower index of 2 (instead of 1 or 0, for instance)?

Answer _____

_____

★**Exercise 4.66.** Compute the following sum, simplifying as much as possible.

$$\sum_{k=1}^{n} k^3 + k =$$

Sometimes double sums are necessary to express a summation. As a general rule, these should be evaluated from the inside out.

Example 4.67. Evaluate the double sum $\sum_{i=1}^{n}\sum_{j=1}^{n} 1$.

Solution: We have $\sum_{i=1}^{n}\sum_{j=1}^{n} 1 = \sum_{i=1}^{n} n = n \cdot n = n^2$.

★**Exercise 4.68.** Evaluate the following double sums

(a) $\sum_{i=1}^{n}\sum_{j=1}^{i} 1 =$

(b) $\sum_{i=1}^{n}\sum_{j=1}^{i} j =$

(c) $\sum_{i=1}^{n}\sum_{j=1}^{n} ij =$

There is a formula for the sum of a geometric sequence, sometimes referred to as a *geometric*

series. It is given in the next theorem.

Theorem 4.69. *Let $x \neq 1$. Then*

$$\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x} \qquad \left(\text{or} \quad \frac{x^{n+1}-1}{x-1} \quad \text{if you prefer} \right).$$

Proof: *First, let $S = \sum_{k=0}^{n} x^k$. Then*

$$xS = x\sum_{k=0}^{n} x^k = \sum_{k=0}^{n} x^{k+1} = \sum_{k=1}^{n+1} x^k.$$

So

$$\begin{aligned} xS - S &= \sum_{k=1}^{n+1} x^k - \sum_{k=0}^{n} x^k \\ &= (x_1 + x_2 + \ldots + x_n + x_{n+1}) - (x_0 + x_1 + \ldots + x_n) \\ &= x^{n+1} - x^0 = x^{n+1} - 1. \end{aligned}$$

So we have $(x-1)S = x^{n+1} - 1$, so $S = \frac{x^{n+1}-1}{x-1}$, since $x \neq 1$. □

Example 4.70.

$$\sum_{k=0}^{n} 3^k = \frac{1-3^{n+1}}{1-3} = \frac{1-3^{n+1}}{-2} = \frac{3^{n+1}-1}{2}.$$

Example 4.71.

$$\sum_{k=0}^{n} \frac{1}{5^k} = \sum_{k=0}^{n} \frac{1^k}{5^k} = \sum_{k=0}^{n} \left(\frac{1}{5}\right)^k = \frac{1-(1/5)^{n+1}}{1-1/5} = \frac{1-1/(5^{n+1})}{4/5} = \frac{5}{4}\left(1 - \frac{1}{5^{n+1}}\right) = \frac{5}{4} - \frac{1}{4 \cdot 5^n}.$$

★**Exercise 4.72.** Find the sum of the following geometric series.
$1 + 3 + 3^2 + 3^3 + \cdots + 3^{49} =$

★**Exercise 4.73.** Find the sum of the following geometric series.
$1 - 2 + 4 - 8 + \cdots - 2^{33} + 2^{34} =$

★**Exercise 4.74.** Find the sum of the following geometric series. Assume $y \neq 1$.

(a) $1 + y + y^2 + y^3 + \cdots + y^{100} =$

(b) $1 - y + y^2 - y^3 + y^4 - y^5 + \cdots - y^{99} + y^{100} =$

(c) $1 + y^2 + y^4 + y^6 + \cdots + y^{100} =$

Corollary 4.75. *Let $N \geq 2$ be an integer. Then*

$$x^N - 1 = (x-1)(x^{N-1} + x^{N-2} + \cdots + x + 1).$$

Proof: *Plugging $N = n + 1$ in the formula from Theorem 4.69 and doing a little algebra yields the formula.* □

Example 4.76. We can see that

$$\begin{aligned} x^2 - 1 &= (x-1)(x+1) \\ x^3 - 1 &= (x-1)(x^2+x+1), \text{ and} \\ x^4 - 1 &= (x-1)(x^3+x^2+x+1). \end{aligned}$$

★**Exercise 4.77.** Factor $x^5 - 1$.

$x^5 - 1 =$_____

Let's use the technique from the proof of Theorem 4.69 in the special case where $x = 2$.

★**Fill in the details 4.78.** Find the sum

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n.$$

Solution: We could just use the formula from Theorem 4.69, but that would be boring. Instead, let's work it out. Let $S = 2^0 + 2^1 + 2^2 + 2^3 + \cdots + 2^n$. Then

$2S =$ _____. Notice S and $2S$ have most of the same terms,

except S has _____ that $2S$ doesn't have and $2S$ has _____ that S doesn't have. Therefore,

$$\begin{aligned} S = 2S - S &= (2^1 + 2^2 + 2^3 + \cdots + 2^n + 2^{n+1}) \\ &\quad -(2^0 + 2^1 + 2^2 + 2^3 + \cdots + 2^n) \\ &= \text{\_\_\_\_\_} \\ &= 2^{n+1} - 1. \end{aligned}$$

Thus, $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

Since powers of 2 are very prominent in computer science, you should definitely commit the formula from the previous example to memory.

Together, Theorems 4.43 and 4.69 imply the following:

Theorem 4.79. *Let $r \neq 1$. Then* $\sum_{k=0}^{n} ar^k = \frac{a - ar^{n+1}}{1 - r}$.

★**Fill in the details 4.80.** Use Theorems 4.43 and 4.69 to prove Theorem 4.79.

Proof: It is easy to see that

$$\sum_{k=0}^{n} ar^k = \qquad = \qquad = \frac{a - ar^{n+1}}{1 - r}.$$

□

★**Exercise 4.81.** Prove Theorem 4.79 *without using Theorems 4.43 and 4.69.* In other words, mimic the proof of Theorem 4.69.

Notice that if $|r| < 1$ then r^n gets closer to 0 the larger n gets. More formally, if $|r| < 1$, $\lim_{n\to\infty} r^n = 0$. This implies the following (which we will not formally prove beyond what we have already said here).

Theorem 4.82. *Let $|r| < 1$. Then*

$$\sum_{k=0}^{\infty} ar^k = \frac{a}{1-r}.$$

Example 4.83. A fly starts at the origin and goes 1 unit up, 1/2 unit right, 1/4 unit down, 1/8 unit left, 1/16 unit up, etc., *ad infinitum.* In what coordinates does it end up?

Solution: Its x coordinate is

$$\frac{1}{2} - \frac{1}{8} + \frac{1}{32} - \cdots = \frac{1}{2}\left(-\frac{1}{4}\right)^0 + \frac{1}{2}\left(-\frac{1}{4}\right)^1 + \frac{1}{2}\left(-\frac{1}{4}\right)^2 + \cdots = \frac{\frac{1}{2}}{1-\frac{-1}{4}} = \frac{2}{5}.$$

Its y coordinate is

$$1 - \frac{1}{4} + \frac{1}{16} - \cdots = \left(-\frac{1}{4}\right)^0 + \left(-\frac{1}{4}\right)^1 + \left(-\frac{1}{4}\right)^2 + \cdots = \frac{1}{1-\frac{-1}{4}} = \frac{4}{5}.$$

Therefore, the fly ends up in $\left(\frac{2}{5}, \frac{4}{5}\right)$.

The following infinite sums are sometimes useful.

Theorem 4.84. *Let $x \in \mathbb{R}$. The following expansions hold:*

$$\begin{aligned}
\sin x &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!} &&= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \cdots \\
\cos x &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} &&= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + \cdots \\
e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n!} &&= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \cdots \\
\frac{1}{1-x} &= \sum_{n=0}^{\infty} x^n &&= 1 + x + x^2 + x^3 + \cdots, \text{ if } |x| < 1
\end{aligned}$$

Product notation is very similar to sum notation, except we multiply the terms instead of adding them.

Definition 4.85. *Let $\{a_n\}$ be a sequence. Then for $1 \le m \le n$, where m and n are integers, we define*

$$\prod_{k=m}^{n} a_k = a_m a_{m+1} \cdots a_n.$$

As with sums, we call k the **index** *and m and n the* **lower limit** *and* **upper limit**, *respectively.*

Example 4.86. Notice that $n! = \prod_{k=1}^{n} k$.

Note: *An alternative way to express the variable and limits of sums and products is*

$$\sum_{m \le k \le n} a_k \qquad \textit{instead of} \qquad \sum_{k=m}^{n} a_k$$

and

$$\prod_{m \le k \le n} a_k \qquad \textit{instead of} \qquad \prod_{k=m}^{n} a_k$$

4.3 Matrices and Matrix Operations

4.3.1 Definitions

Definition 4.87. *An $m \times n$ (read m by n)* **matrix** *A with m rows and n columns with entries over $\mathbb{R}$ is a rectangular array of the form*

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},$$

where $\forall (i,j) \in \{1,2,\ldots,m\} \times \{1,2,\ldots,n\}, \quad a_{ij} \in \mathbb{R}$.
The number of rows and columns of a matrix is referred to as its **dimensions**.

Example 4.88. $A = \begin{bmatrix} 0 & 4 & 1 \\ 1 & 2 & 3 \end{bmatrix}$ is a 2×3 mtrix and $B = \begin{bmatrix} -2 & 1 \\ 1 & 2 \\ 0 & 3 \end{bmatrix}$ is a 3×2 matrix.

Note: *As a shortcut, we use the notation $A = [a_{ij}]$ to denote the matrix A with entries a_{ij}.*

Note: *In most programming languages, matrices are indexed starting with 0 instead of 1. So the row indices go from 0 to $m-1$ and the column indices go from 0 to $n-1$. There is a very good technical reason for this, but we will not worry about that for now. We will stick with a starting index of 1 in these notes since in mathematics that is more common.*

Definition 4.89. *To refer to a specific entry of a matrix, we use the notation a_{ij} (without square brackets). Sometimes we use a comma, as in $a_{i,j}$, to separate the two subscripts. Alternatively, the notation $A[i,j]$ or $A[i][j]$ is used, especially in programming languages.*

Example 4.90. If $A = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$, then $a_{2,3} = A[2,3] = A[2][3] = 3$. Also, $A[1,2] = -1$.

Example 4.91. Write out explicitly the 4×4 matrix $A = [a_{ij}]$ where $a_{ij} = i^2 - j^2$.

Solution: $$A = \begin{bmatrix} 1^2-1^1 & 1^2-2^2 & 1^2-3^2 & 1^2-4^2 \\ 2^2-1^2 & 2^2-2^2 & 2^2-3^2 & 2^2-4^2 \\ 3^2-1^2 & 3^2-2^2 & 3^2-3^2 & 3^2-4^2 \\ 4^2-1^2 & 4^2-2^2 & 4^2-3^2 & 4^2-4^2 \end{bmatrix} = \begin{bmatrix} 0 & -3 & -8 & -15 \\ 3 & 0 & -5 & -12 \\ 8 & 5 & 0 & -7 \\ 15 & 12 & 7 & 0 \end{bmatrix}.$$

★**Exercise 4.92.** Write out explicitly the 3×3 matrix $A = [a_{ij}]$ where $a_{ij} = i^j$.

Definition 4.93. *We denote by* $\mathbf{M}_{m\times n}(\mathbb{R})$ *the set of all* $m \times n$ *matrices with entries over* $\mathbb{R}$. *Since we will always be working over* $\mathbb{R}$ *in this book, we will shorthand this notation to* $\mathbf{M}_{m\times n}$. $\mathbf{M}_{n\times n}$ *is, in particular, the set of all square matrices of size* n.

Definition 4.94. *The* $m \times n$ **zero matrix**, $\mathbf{0}_{m\times n} \in \mathbf{M}_{m\times n}$, *is the matrix with* 0*'s everywhere,*

$$\mathbf{0}_{m\times n} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

When $m = n$ *we write* $\mathbf{0}_n$ *as a shortcut for* $\mathbf{0}_{n\times n}$.

Definition 4.95. *The* $n \times n$ **identity matrix**, $\mathbf{I}_n \in \mathbf{M}_{n\times n}$, *is the matrix with* 1*'s on the main diagonal and* 0*'s everywhere else,*

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

★**Exercise 4.96.** Explicitly write out the entries of the matrices $\mathbf{0}_{3\times 4}$ and $\mathbf{I}_5$.

Definition 4.97 (Matrix Addition and Multiplication of a Matrix by a Scalar)**.**
Let $A = [a_{ij}], B = [b_{ij}] \in \mathbf{M}_{m\times n}$ and $\alpha \in \mathbb{R}$.

- *The matrix αA is the matrix $C \in \mathbf{M}_{m\times n}$ with entries $C = [c_{ij}]$ where $c_{ij} = \alpha a_{ij}$.*
- *The matrix $A + B$ is the matrix $C \in \mathbf{M}_{m\times n}$ with entries $C = [c_{ij}]$ where $c_{ij} = a_{ij} + b_{ij}$.*

Example 4.98. Let $A = \begin{bmatrix} 2 & -3 & 1 \\ 4 & -7 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 3 & -5 \\ 6 & 0 & 4 \end{bmatrix}$. Then

$$3A = \begin{bmatrix} 3\times 2 & 3\times -3 & 3\times 1 \\ 3\times 4 & 3\times -7 & 3\times 3 \end{bmatrix} = \begin{bmatrix} 6 & -9 & 3 \\ 12 & -21 & 9 \end{bmatrix}$$

and

$$A + B = \begin{bmatrix} 2+0 & -3+3 & 1-5 \\ 4+6 & -7+0 & 3+4 \end{bmatrix} = \begin{bmatrix} 2 & 0 & -4 \\ 10 & -7 & 7 \end{bmatrix}.$$

★**Exercise 4.99.** Let $A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \\ 0 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 1 \\ 2 & 1 \\ 0 & -1 \end{bmatrix}$. Compute $A + 2B$.

★**Exercise 4.100.** Let $a, b, c \in \mathbb{R}$ and let

$$M = \begin{bmatrix} a & -2a & c \\ 0 & -a & b \\ a+b & 0 & -1 \end{bmatrix}, \qquad N = \begin{bmatrix} 1 & 2a & c \\ a & b-a & -b \\ a-b & 0 & -1 \end{bmatrix}.$$

Compute $M + N$ and $2M$.

The following properties of matrices can easily be proved by applying the definitions of matrix addition and scalar multiplication.

Theorem 4.101. *Let $A, B, C \in \mathbf{M}_{m\times n}$ and $\alpha, \beta \in \mathbb{R}$. Then*

1. *$\mathbf{M}_{m\times n}$ is closed under matrix addition and scalar multiplication*

$$A + B \in \mathbf{M}_{m\times n}, \qquad \alpha A \in \mathbf{M}_{m\times n} \tag{4.1}$$

2. *Addition of matrices is commutative*

$$A + B = B + A \tag{4.2}$$

3. *Addition of matrices is associative*

$$A + (B + C) = (A + B) + C \tag{4.3}$$

4. *The zero matrix is the additive identity*

$$A + \mathbf{0}_{m\times n} = A \tag{4.4}$$

5. *Additive inverse*

$$A + (-A) = (-A) + A = \mathbf{0}_{m\times n} \tag{4.5}$$

6. *Distributive law*

$$\alpha(A + B) = \alpha A + \alpha B \tag{4.6}$$

7. *Distributive law*
$$(\alpha+\beta)A = \alpha A + \beta A \tag{4.7}$$

8. *Scalar multiplicative identity*
$$1A = A \tag{4.8}$$

9.
$$\alpha(\beta A) = (\alpha\beta)A \tag{4.9}$$

★**Exercise 4.102.** Determine x and y such that
$$\begin{bmatrix} 3 & x & 1 \\ 1 & 2 & 0 \end{bmatrix} + 2\begin{bmatrix} 2 & 1 & 3 \\ 5 & x & 4 \end{bmatrix} = \begin{bmatrix} 7 & 3 & 7 \\ 11 & y & 8 \end{bmatrix}.$$

4.3.2 Matrix Multiplication

Matrix multiplication is more straightforward that the following definition makes it seem. Once you have a little practice with it, it comes very naturally.

Definition 4.103. *Let $A = [a_{ij}] \in \mathbf{M}_{m\times n}$ and $B = [b_{ij}] \in \mathbf{M}_{n\times p}$. Then the matrix product AB is defined as the matrix $C = [c_{ij}] \in \mathbf{M}_{m\times p}$ with entries $c_{ij} = \sum_{l=1}^{n} a_{il}b_{lj}$:*

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1p} \\ b_{21} & \cdots & b_{2j} & \cdots & b_{2p} \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ b_{n1} & \cdots & b_{nj} & \cdots & b_{np} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1p} \\ c_{21} & \cdots & c_{2p} \\ \vdots & \ldots & \vdots \\ \cdots & c_{ij} & \cdots \\ \vdots & \ldots & \vdots \\ c_{m1} & \cdots & c_{mp} \end{bmatrix}.$$

Note:

1. *Observe that we use juxtaposition rather than a special symbol to denote matrix multiplication. This will simplify notation.*

2. *In order to obtain the ij-th entry of the matrix AB we multiply element-wise the i-th row of A by the j-th column of B.*

3. *Observe that AB is a $m \times p$ matrix, and that in order to multiply two matrices, the number of columns of the first matrix must be equal to the number of rows of the second one.*

Example 4.104. Let $M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $N = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$. Then

$$MN = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{bmatrix} = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix},$$

and

$$NM = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 5 \cdot 1 + 6 \cdot 3 & 5 \cdot 2 + 6 \cdot 4 \\ 7 \cdot 1 + 8 \cdot 3 & 7 \cdot 2 + 8 \cdot 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}.$$

Notice that matrix multiplication is not necessarily commutative!

★**Exercise 4.105.** Consider the matrix

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 0 & 1 & 1 \\ 4 & 4 & 0 \end{bmatrix}.$$

Compute AA.

Example 4.106. Notice that

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Observe then that the product of two non-zero matrices may be the zero matrix.

★**Exercise 4.107.** Let $a, b, c \in \mathbb{R}$, $A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, and $B = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$. Find AB and BA.

Even though matrix multiplication is not necessarily commutative, it is associative.

Theorem 4.108. *If $A \in \mathbf{M}_{m\times n}, B \in \mathbf{M}_{n\times r}$, and $C \in \mathbf{M}_{r\times s}$ then*

$$(AB)C = A(BC),$$

i.e., matrix multiplication is associative.

> **Proof:** *To prove this we only need to consider the ij-th entry of each side, appeal to the associativity of mulitplication of real numbers, and verify that both sides are indeed equal to*
>
> $$\sum_{k=1}^{n}\sum_{k'=1}^{r} a_{ik}b_{kk'}c_{k'j}.$$
>
> □

Definition 4.109. *Let $A \in \mathbf{M}_{n\times n}$. The notation A^k has the obvious meaning of k copies of A multiplied together. We can define it more formally as $A^k = AA^{k-1}$ if $k > 1$.*

Note: *By virtue of associativity, a square matrix commutes with its powers, that is, if $A \in \mathbf{M}_{n\times n}$, and $r, s \in \mathbb{N}$, then $(A^r)(A^s) = (A^s)(A^r) = A^{r+s}$.*

★**Exercise 4.110.** Let $M = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$. Find M^6. (Hint: If you are clever, you can do this with 3 multiplications instead of 5!)

Example 4.111. Let $A \in \mathbf{M}_{3\times 3}$ be given by

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

We will demonstrate, using a technique called induction, that $A^n = 3^{n-1}A$ for $n \in \mathbb{N}, n \geq 1$.

Solution: The assertion is trivial for $n = 1$. Assume its truth for $n-1$, that is, assume $A^{n-1} = 3^{n-2}A$. Observe that

$$A^2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix} = 3A.$$

Now

$$A^n = AA^{n-1} = A(3^{n-2}A) = 3^{n-2}A^2 = 3^{n-2}3A = 3^{n-1}A,$$

and so the assertion is proved by induction.

Do not worry if you do not fully buy into this proof at this point. Although it may appear we used circular reasoning here, we in fact did not. All will be explained in the section on induction later. But we couldn't resist including this example as a foreshadowing of things to come!

Theorem 4.112. *There is a unique matrix $E \in \mathbf{M}_{n\times n}$ such that for every $A \in \mathbf{M}_{n\times n}$, $AE = EA = A$. In particular, that matrix is $E = \mathbf{I}_n$, the identity matrix.*

Proof: *It is clear that for any $A \in \mathbf{M}_{n\times n}$, $A\mathbf{I}_n = \mathbf{I}_n A = A$. Now because E is*

an identity, $E\mathbf{I}_n = \mathbf{I}_n$. *Because* $\mathbf{I}_n$ *is an identity,* $E\mathbf{I}_n = E$. *Whence*

$$\mathbf{I}_n = E\mathbf{I}_n = E,$$

demonstrating uniqueness. □

Note: *The fact that* $\mathbf{I}_n$ *is the multiplicative identity of* $\mathbf{M}_{n\times n}$ *(much like 1 is the multiplicative identity of real numbers) is the reason we call it the identity matrix.*

Example 4.113. Let $A = [a_{ij}] \in \mathbf{M}_{n\times n}$ be such that $a_{ij} = 0$ for $i > j$ and $a_{ij} = 1$ if $i \leq j$. Find A^2.

Solution: Let $A^2 = B = [b_{ij}]$. Then

$$b_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}.$$

Observe that the i-th row of A has $i-1$ 0's followed by $n-i+1$ 1's, and the j-th column of A has j 1's followed by $n-j$ 0's. Therefore if $i-1 > j$, then $b_{ij} = 0$. If $i \leq j+1$, then

$$b_{ij} = \sum_{k=i}^{j} a_{ik}a_{kj} = j - i + 1.$$

This means that

$$A^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ 0 & 1 & 2 & 3 & \cdots & n-2 & n-1 \\ 0 & 0 & 1 & 2 & \cdots & n-3 & n-2 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Example 4.114. Let x be a real number, and let

$$m(x) = \begin{bmatrix} 1 & 0 & x \\ -x & 1 & -\dfrac{x^2}{2} \\ 0 & 0 & 1 \end{bmatrix}.$$

If a, b are real numbers, prove that

1. $m(a)m(b) = m(a+b)$.
2. $m(a)m(-a) = \mathbf{I}_3$, the 3×3 identity matrix.

Solution: For the first part, observe that

$$\begin{aligned} m(a)m(b) &= \begin{bmatrix} 1 & 0 & a \\ -a & 1 & -\frac{a^2}{2} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & b \\ -b & 1 & -\frac{b^2}{2} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a+b \\ -a-b & 1 & -\frac{a^2}{2} - \frac{b^2}{2} + ab \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & a+b \\ -(a+b) & 1 & -\frac{(a+b)^2}{2} \\ 0 & 0 & 1 \end{bmatrix} = m(a+b) \end{aligned}$$

For the second part, observe that using the preceding part of the problem,

$$m(a)m(-a) = m(a-a) = m(0) = \begin{bmatrix} 1 & 0 & 0 \\ -0 & 1 & -\frac{0^2}{2} \\ 0 & 0 & 1 \end{bmatrix} = \mathbf{I}_3,$$

giving the result.

★**Exercise 4.115.** A square matrix X is called *idempotent* if $X^2 = X$. Prove that if $AB = A$ and $BA = B$ then A and B are idempotent.

★**Exercise 4.116.** Prove or disprove: If $A, B \in \mathbf{M}_{n\times n}$ are such that $AB = \mathbf{0}_n$, then also $BA = \mathbf{0}_n$. Hint: Play around with some simple 2×2 matrices.

4.3.3 Trace and Transpose

Definition 4.117. *Let $A = [a_{ij}] \in \mathbf{M}_{n\times n}$. Then the* trace *of A, denoted by $\operatorname{tr}(A)$ is the sum of the diagonal elements of A. That is,*

$$\operatorname{tr}(A) = \sum_{k=1}^{n} a_{kk}.$$

Theorem 4.118. *Let $A = [a_{ij}] \in \mathbf{M}_{n\times n}, B = [b_{ij}] \in \mathbf{M}_{n\times n}$. Then*

$$\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B), \tag{4.10}$$

$$\operatorname{tr}(AB) = \operatorname{tr}(BA). \tag{4.11}$$

Proof: *The first assertion is trivial. To prove the second, observe that $AB = (\sum_{k=1}^{n} a_{ik}b_{kj})$ and $BA = (\sum_{k=1}^{n} b_{ik}a_{kj})$. Then*

$$\operatorname{tr}(AB) = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik} = \operatorname{tr}(BA),$$

whence the theorem follows. □

Example 4.119. Let A, B be square matrices of size $n > 0$. Is it possible that $AB - BA = \mathbf{I}_n$? Prove or disprove!

Solution: This is impossible. Consider taking traces on both sides:

$$0 = \operatorname{tr}(AB) - \operatorname{tr}(BA) = \operatorname{tr}(AB - BA) = \operatorname{tr}(\mathbf{I}_n) = n$$

which is a contradiction, since $n > 0$.

★**Exercise 4.120.** Consider the matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M}_{2\times 2}$. Find necessary and sufficient conditions on a, b, c, d so that $\operatorname{tr}\left(A^2\right) = (\operatorname{tr}(A))^2$.

Definition 4.121. *The* transpose *of a matrix* $A = [a_{ij}] \in \mathbf{M}_{m\times n}$ *is the matrix* $A^T = B = [b_{ij}] \in \mathbf{M}_{n\times m}$, *where* $b_{ij} = a_{ji}$.

Example 4.122. If $M = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$, then $M^T = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$.

★**Exercise 4.123.** Find N^T if $N = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{bmatrix}$.

Theorem 4.124. *Let*

$$A = [a_{ij}] \in \mathbf{M}_{m\times n},\ B = [b_{ij}] \in \mathbf{M}_{m\times n},\ C = [c_{ij}] \in \mathbf{M}_{n\times r},\ \alpha \in \mathbb{R}, u \in \mathbb{N}.$$

Then

$$A^{TT} = A, \tag{4.12}$$

$$(A + \alpha B)^T = A^T + \alpha B^T, \tag{4.13}$$

$$(AC)^T = C^T A^T, \tag{4.14}$$

$$(A^u)^T = (A^T)^u. \tag{4.15}$$

Proof: *The first two assertions are obvious, and the fourth follows from the third by using induction. To prove the third put* $A^T = (\alpha_{ij})$, $\alpha_{ij} = a_{ji}$, $C^T = (\gamma_{ij})$, $\gamma_{ij} = c_{ji}$, $AC = (u_{ij})$ *and* $C^T A^T = (v_{ij})$. *Then*

$$u_{ij} = \sum_{k=1}^{n} a_{ik}c_{kj} = \sum_{k=1}^{n} \alpha_{ki}\gamma_{jk} = \sum_{k=1}^{n} \gamma_{jk}\alpha_{ki} = v_{ji},$$

whence the theorem follows. □

Definition 4.125. *A square matrix* $A \in \mathbf{M}_{n\times n}$ *is* symmetric *if* $A^T = A$. *A matrix* $B \in \mathbf{M}_{n\times n}$ *is* skew-symmetric *if* $B^T = -B$.

Example 4.126. Let A, B be square matrices of the same size, with A symmetric and B skew-symmetric. Prove that the matrix A^2BA^2 is skew-symmetric.

Solution: We have

$$(A^2BA^2)^T = (A^2)^T(B)^T(A^2)^T = A^2(-B)A^2 = -A^2BA^2.$$

★**Exercise 4.127.** Let A, B be square matrices of the same size, with A symmetric and B skew-symmetric. Prove that the matrix $AB - BA$ is symmetric.

4.4 Reading Comprehension Questions

From Section 4.1

★**Question 4.1.** If $\{x_n\}$ is defined by $x_n = 3^n - 2^n$, find x_1, x_2, x_3, x_4, and x_5.

★**Question 4.2.** What does it mean to *solve* a recurrence relation?

★**Question 4.3.** If $\{x_n\}$ is defined by $x_1 = 1$ and $x_n = 2x_{n-1} + 3$, find x_2, x_3, x_4, and x_5.

★**Question 4.4.** Let $\{x_n\}$ be defined by $x_1 = 2$ and $x_n = x_{n-1} + 3$.

(a) Find x_2, x_3, x_4, and x_5.

(b) Find a closed form for x_n.

(c) Prove that your closed form is correct by following the technique from Example 4.11.

★**Question 4.5.** Are geometric progressions always, sometime, or never monotonic? Explain. Similarly, are they always, sometimes, or never increasing?

★**Question 4.6.** Are arithmetic progressions always, sometime, or never monotonic? Explain. Similarly, are they always, sometimes, or never increasing?

★**Question 4.7.** Give an example (not from the book) of each of the following.

(a) A geometric progression in closed form.

(b) An arithmetic progression in closed form.

(c) A recurrence relation that defines a geometric progression.

(d) A recurrence relation that defines an arithmetic progression.

From Section 4.2

★**Question 4.8.** Are $\sum_{i=1}^{n} -x^i$ and $\sum_{i=1}^{n} (-x)^i$ the same? Explain.

★**Question 4.9.** Write $-1 + 3 - 9 + 27 - 81 + 243 - 729$ using a summation.

★**Question 4.10.** Compute $\sum_{k=0}^{30} 5k - 7$.

★**Question 4.11.** Compute $\sum_{k=0}^{n} 2^k$. (Eventually you will hopefully have this one memorized.)

★**Question 4.12.** Is it ever the case that $\sum_{i=0}^{n} x_i = \sum_{i=1}^{n} x_i$? If so, when? Give an example.

★**Question 4.13.** Compute $\sum_{k=1}^{23} \frac{11}{(-7)^k}$. Simplify your answer (although you don't need to compute the actual number). (I have thrown several subtle tricks at you on this one, but if you read carefully and apply what you know, you should be able to do it!)

★**Question 4.14.** Estimate cos(1) without using a calculator.

From Section 4.3.1

★**Question 4.15.** Can you add a 3×4 matrix to a 4×3 matrix? Explain.

★**Question 4.16.** Write out the 4×3 matrix $A = [a_{ij}]$ where $a_{ij} = 2^{i-1}3^{j-1}$.

★**Question 4.17.** Let $A = \begin{bmatrix} -3 & 0 & 1 \\ 4 & -2 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 7 & -5 \\ 7 & 1 & 8 \end{bmatrix}$. Compute $3A$ and $A - B$.

★**Question 4.18.** Explicitly write out the entries of the matrices $\mathbf{0}_{2\times 5}$ and $\mathbf{I}_3$.

From Section 4.3.2

★**Question 4.19.** Can you multiply a 3×4 matrix by a 4×7 matrix? What about multiplying a 6×3 matrix by a 6×3 matrix. If you can, what are the dimensions of the result? If you can't, explain why not.

★**Question 4.20.** Determine the product $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -2 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.

★**Question 4.21.** Let A be a $n \times n$ matrix such that $A^5 = \mathbf{0}_n$. What is A^{19}?

★**Question 4.22.** Find all real numbers x such that

$$\begin{bmatrix} -4 & x \\ -x & 4 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

★**Question 4.23.** Prove or disprove: For all matrices $A, B \in \mathbf{M}_{n\times n}$, $(A + B)(A - B) = A^2 - B^2$. Hint: Play around with some simple 2×2 matrices.

From Section 4.3.3

★**Question 4.24.** Let $A, B \in \mathbf{M}_{2\times 2}$ be symmetric matrices. Must their product AB be symmetric? Prove or disprove!

★**Question 4.25.** Prove or disprove: If A, B are square matrices of the same size, then it is always true that $\operatorname{tr}(AB) = \operatorname{tr}(A)\operatorname{tr}(B)$.

★**Question 4.26.** Let A be a square matrix. Prove that the matrix AA^T is symmetric.

4.5 Problems

Problem 4.1. Find at least three *different* sequences that begin with 1, 3, 7 whose terms are generated by a simple formula or rule. By different, I mean none of the sequences can have exactly the same terms. In other words, your answer cannot simply be three different ways to generate the same sequence.

Problem 4.2. Let $q_n = 2q_{n-1} + 2n + 5$, and $q_0 = 0$. Compute q_1, q_2, q_3 and q_4.

Problem 4.3. Let $a_n = a_{n-2} + n$, $a_0 = 0$, and $a_1 = 1$. Compute a_2, a_3, a_4 and a_5.

Problem 4.4. Let $a_n = n \times a_{n-1} + 5$, and $a_0 = 1$. Compute a_1, a_2, a_3, a_4 and a_5.

Problem 4.5. Define a sequence $\{x_n\}$ by $x_0 = 1$, and $x_n = 2x_{n-1} + 1$ if $n \geq 1$. Find a closed form for the nth term of this sequence. *Prove that your solution is correct.*

Problem 4.6. Compute each of the following:

(a) $\displaystyle\sum_{k=5}^{40} k$

(b) $\displaystyle\sum_{j=5}^{22} (2^{j+1} - 2^j)$

(c) $\displaystyle\sum_{k=0}^{n} 5k$

(d) $\displaystyle\sum_{i=1}^{3}\sum_{j=1}^{4} j$

(e) $\displaystyle\sum_{k=1}^{n} k(k-1)$

(f) $\displaystyle\sum_{j=1}^{n} 5^j$

(g) $\displaystyle\sum_{j=0}^{\log_2 n} 2^j$

(h) $\displaystyle\sum_{i=0}^{\log_2 n} \left(\frac{n}{2^i}\right)$

(i) $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{i}\sum_{k=1}^{j} 1$

Problem 4.7. Here is a standard interview question for prospective computer programmers: You are given a list of $1,000,001$ positive integers from the set $\{1, 2, \ldots, 1,000,000\}$. In the list, every member of $\{1, 2, \ldots, 1,000,000\}$ is listed once, except for x, which is listed twice, and the numbers are listed in some unknown order. How do you find what x is without doing a $1,000,000$ step search (e.g. check if 1 is on the list twice, then check if 2 is on the list twice, etc.)? How much faster is your solution than the naive solution?

Problem 4.8. Find a closed formula for

$$T_n = 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2.$$

Problem 4.9. Show that when $n \geq 1$,

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Problem 4.10. Assuming $n \geq 1$, find and prove a closed formula for

$$2 + 4 + 6 + \cdots + 2n$$

Problem 4.11. Show that when $n \geq 1$,

$$\sum_{k=1}^{n} \frac{k}{k^4 + k^2 + 1} = \frac{1}{2} \cdot \frac{n^2 + n}{n^2 + n + 1}.$$

Problem 4.12. Legend says that the inventor of the game of chess, Sissa ben Dahir, asked the King Shirham of India to place a grain of wheat on the first square of the chessboard, 2 on the second square, 4 on the third square, 8 on the fourth square, etc..

(a) How many grains of wheat are to be put on the last (64-th) square?

(b) How many grains, total, are needed in order to satisfy the greedy inventor?

(c) Given that 15 grains of wheat weigh approximately one gram, what is the approximate weight, in kg, of the wheat needed?

(d) Given that the annual production of wheat is 350 million tonnes, how many years, approximately, are needed in order to satisfy the inventor (assume that production of wheat stays constant)?

Problem 4.13. Find a closed formula for $\sum_{k=1}^{n} k^2(k-1)$. Simplify the formula as much as possible.

Problem 4.14. Find a closed formula for $\sum_{k=1}^{n} k \cdot k!$. (Hint: What is $(k+1)! - k!$, and why does it matter?) Simplify the formula as much as possible.

Problem 4.15. Prove that for $n \geq 1$, $\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$.

Problem 4.16. Write out explicitly the 3×3 matrix $A = [a_{ij}]$ where $a_{ij} = ij$.

Problem 4.17. Determine 2×2 matrices A and B such that

$$2A - 5B = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \text{ and } -2A + 6B = \begin{bmatrix} 4 & 2 \\ 6 & 0 \end{bmatrix}.$$

Problem 4.18. A person goes along the rows of a movie theater and asks the tallest person of each row to stand up. Then he selects the shortest of these people, who we will call the *shortest giant*. Another person goes along the rows and asks the shortest person to stand up and from these he selects the tallest, which we will call the *tallest dwarf*. Who is taller, the tallest dwarf or the shortest giant? Prove your answer.

Problem 4.19 (Putnam Exam, 1959)**.** Choose five elements from the following matrix, no two coming from the same row or column, so that the minimum of these five elements is as large as possible.

$$\begin{bmatrix} 11 & 17 & 25 & 19 & 16 \\ 24 & 10 & 13 & 15 & 3 \\ 12 & 5 & 14 & 2 & 18 \\ 23 & 4 & 1 & 8 & 22 \\ 6 & 20 & 7 & 21 & 9 \end{bmatrix}$$

Problem 4.20. Find $a + b + c$ if $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{bmatrix} = \begin{bmatrix} a & a & a \\ b & b & b \\ c & c & c \end{bmatrix}$.

Problem 4.21. (Requires calculus) Let

$$A = \begin{bmatrix} 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

Calculate the value of the infinite series

$$\mathbf{I}_3 + A + A^2 + A^3 + \cdots .$$

Problem 4.22. Consider the matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & x \end{bmatrix}$, where x is a real number. Find the value of x such that there are non-zero 2×2 matrices B such that $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Problem 4.23. Let $A \in \mathbf{M}_{l\times m}$, $B, C \in \mathbf{M}_{m\times n}$, and $\alpha \in \mathbb{R}$. Prove that

1. $A(B + C) = AB + AC$,
2. $(A + B)C = AC + BC$, and
3. $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

Problem 4.24. A matrix $A = [a_{ij}] \in \mathbf{M}_{n\times n}$ is said to be *checkered* if $a_{ij} = 0$ when $(j - i)$ is odd. Prove that the sum and the product of two checkered matrices is checkered.

Problem 4.25. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Demonstrate that $A^2 - (a + d)A + (ad - bc)\mathbf{I}_2 = \mathbf{0}_2$.

Problem 4.26. Let $A \in \mathbf{M}_{2\times 2}$ and let $k \in \mathbb{Z}, k > 2$. Prove that $A^k = \mathbf{0}_2$ if and only if $A^2 = \mathbf{0}_2$. (Hint: Use Problem 4.25.)

Problem 4.27. Find all matrices $A \in \mathbf{M}_{2\times 2}$ such that $A^2 = \mathbf{0}_2$

Problem 4.28. Find all matrices $A \in \mathbf{M}_{2\times 2}$ such that $A^2 = \mathbf{I}_2$

Problem 4.29. Find a solution $X \in \mathbf{M}_{2\times 2}$ for

$$X^2 - 2X = \begin{bmatrix} -1 & 0 \\ 6 & 3 \end{bmatrix}.$$

Problem 4.30. Find, with proof, a 4×4 **non-zero** matrix A such that

$$A \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Problem 4.31. Let X be a 2×2 matrices with real number entries. Solve the equation

$$X^2 + X = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

(that means find *all* solutions.)

Problem 4.32. Write

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

as the sum of two 3×3 matrices $\mathbf{E}_1, \mathbf{E}_2$, with $\operatorname{tr}(\mathbf{E}_2) = 10$.

Problem 4.33. Give an example of two matrices $A, B \in \mathbf{M}_{2\times 2}$ that *simultaneously* satisfy the following properties:

1. $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $B \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.
2. $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.
3. $\operatorname{tr}(A) = \operatorname{tr}(B) = 2$.
4. $A = A^T$ and $B = B^T$.

Problem 4.34. Prove that there are no matrices $A, B, C, D \in \mathbf{M}_{n\times n}$ such that $AC + DB = \mathbf{I}_n$ and $CA + BD = \mathbf{0}_n$.

Problem 4.35. Given square matrices $A, B \in \mathbf{M}_{7\times 7}$ such that $\operatorname{tr}\left(A^2\right) = \operatorname{tr}\left(B^2\right) = 1$, and $(A - B)^2 = 3\mathbf{I}_7$, find $\operatorname{tr}(BA)$.

Problem 4.36. Given a square matrix $A \in \mathbf{M}_{4\times 4}$ such that $\operatorname{tr}\left(A^2\right) = -4$, and

$$(A - \mathbf{I}_4)^2 = 3\mathbf{I}_4,$$

find $\operatorname{tr}(A)$. Hint: Start by computing $\operatorname{tr}\left((A - \mathbf{I}_4)^2\right)$.

Problem 4.37. Prove or disprove: If $A, B, C \in \mathbf{M}_{3\times 3}$ then $\operatorname{tr}(ABC) = \operatorname{tr}(BAC)$.

Problem 4.38. Let $A \in \mathbf{M}_{n\times n}, A = [a_{ij}]$. Prove that $\operatorname{tr}\left(AA^T\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2$.

Problem 4.39. Let $X \in \mathbf{M}_{n\times n}$. Prove that if $XX^T = \mathbf{0}_n$ then $X = \mathbf{0}_n$.

Chapter 5: Recurrences and Induction

In this chapter we bring together three foundational tools in the study of discrete mathematics:

1. **Asymptotic notation and growth rates**, which give us a concise way to compare the size of functions. We will introduce the most common asymptotic notations (O, Θ, Ω, and o), and work through examples comparing logarithmic, polynomial, and exponential rates of growth.

2. **Recurrence relations**, a means of defining a sequence a_n by expressing each term in terms of earlier ones. We will develop several methods for solving recurrences.

3. **Mathematical induction**, the principal proof technique for establishing that a statement holds for all integers above a base value. We will use mathematical induction to verify closed-form solutions of recurrences, to prove properties of asymptotic notation, and to tackle a variety of proofs about sequences.

5.1 Asymptotic Notation

Asymptotic notation is used to express and compare the growth rate of functions. We will define the asymptotic notations in terms of nonnegative functions. You will find more general definitions of these notations in other books, but they are more complicated, more difficult to understand, and harder to work with. These added difficulties are a result of the possibility of the functions involved being negative. But in many contexts, the functions of interest are nonnegative, so restricting our attention to such functions is fine.

Asymptotic notation allows us to express the behavior of a function as the input approaches infinity. In other words, it is concerned about what happens to $f(n)$ as n gets larger, and is not concerned about the value of $f(n)$ for small values of n.

We will define four of the most commonly used notations (an allude to the definition of a fifth), providing a few brief examples of each. We will then discuss some of the most important and useful properties of these notations. Finally, we will present many more detailed examples.

5.1.1 The Notations

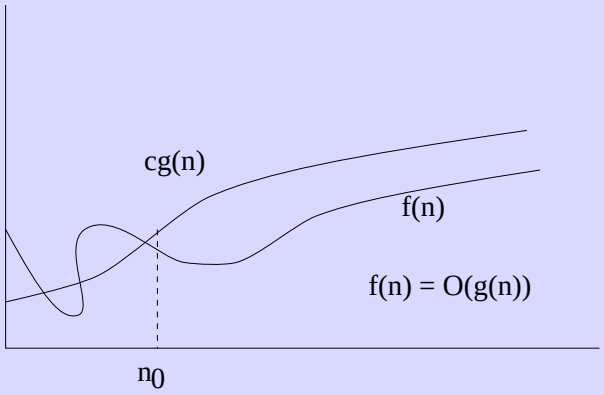
We begin with the most commonly used of the notations: *Big-O (O)*. We will define it and give several examples of its use. We will then present *Big-Omega (Ω)*, *Big-Theta (Θ)*, and little-o (o) notations, providing definitions and examples, and discussing how the notations relate to each other.

Definition 5.1 (Big-O)**.** *Let f be a nonnegative function.*

We say that $f(n)$ is **Big-O** *of $g(n)$, written as $f(n) = O(g(n))$, iff there are positive constants c and n_0 such that*

$$f(n) \leq c\, g(n) \text{ for all } n \geq n_0.$$

If $f(n) = O(g(n))$, $f(n)$ grows no faster than $g(n)$. In other words, $g(n)$ is an **asymptotic upper bound** *(or just* **upper bound***) on $f(n)$.*



Note: *The "=" in the statement "$f(n) = O(g(n))$" should be read and thought of as "is", not "equals." You can think of it as a one-way equals. So saying $f(n) = O(g(n))$ is* not *the same thing as saying $O(g(n)) = f(n)$, for instance (with the latter statement not really making sense).*

An alternative notation is to write $f(n) \in O(g(n))$ instead of $f(n) = O(g(n))$. It turns out that $O(g(n))$ is actually the set of all functions that grow no faster than $g(n)$, so the set notation is actually in some sense more correct. The "=" notation is used because it comes in handy when doing algebra. You can essentially think of these as being two different notations ($=$ and $\in$) for the same thing. Similar statements are true for the other asymptotic notations.

Example 5.2. Prove that $n^2 + n = O(n^3)$.

Solution: Here, we have $f(n) = n^2 + n$, and $g(n) = n^3$. Notice that if $n \geq 1$, $n \leq n^3$ and $n^2 \leq n^3$. Therefore,

$$n^2 + n \leq n^3 + n^3 = 2n^3$$

Thus,

$$n^2 + n \leq 2n^3 \text{ for all } n \geq 1.$$

Thus, we have shown that $n^2 + n = O(n^3)$ by definition of Big-O, with $n_0 = 1$, and $c = 2$.

The following fact is a generalization of what was used in the previous example. It is used often in proofs involving asymptotic notation.

Theorem 5.3. *If a and b are real numbers with $a \leq b$, then $n^a \leq n^b$ whenever $n \geq 1$.*

Proof: *We will not provide a proof, but it should be fairly clear intuitively that this is true. If you cannot see why this is true, you should work out a few examples to convince yourself.* □

Sometimes the easiest way to prove that $f(n) = O(g(n))$ is to take c to be the sum of the *positive* coefficients of $f(n)$, although this trick doesn't always work. We can usually easily eliminate the lower order terms with negative coefficients if we make the appropriate assumption. Let's see how to do this in the next few examples.

Example 5.4. Prove that $3n^3 - 2n^2 + 13n - 15 = O(n^3)$.

Solution: First, notice that if $n \geq 0$, then $-2n^2 - 15 \leq 0$, so

$$3n^3 - 2n^2 + 13n - 15 \leq 3n^3 + 13n.$$

Next, if $n \geq 1$, then $13n \leq 13n^3$. Therefore if $n \geq 1$,

$$3n^3 + 13n \leq 3n^3 + 13n^3 = 16n^3.$$

Also notice that if $n \geq 1$, then $n \geq 0$. Thus, our first step is still valid if we assume $n \geq 1$ since $n \geq 1$ is a stronger condition than $n \geq 0$. Putting this all together, if we assume $n \geq 1$, then

$$\begin{aligned} 3n^3 - 2n^2 + 13n - 15 &\leq 3n^3 + 13n \\ &\leq 3n^3 + 13n^3 \\ &= 16n^3. \end{aligned}$$

Since we have shown that $3n^3 - 2n^2 + 13n - 15 \leq 16n^3$ for all $n \geq 1$, we have proven that $3n^3 - 2n^2 + 13n - 15 = O(n^3)$.

We used $n_0 = 1$ and $c = 16$ in our proof. It is not necessary to explicitly point this out in our proof, though. We only do so to help you see the connection between the proof and the definition of Big-O.

Example 5.5. Prove that $5n^2 - 3n + 20 = O(n^2)$.

Solution: If $n \geq 1$,

$$\begin{aligned} 5n^2 - 3n + 20 &\leq 5n^2 + 20 && (5.1) \\ &\leq 5n^2 + 20n^2 && (5.2) \\ &= 25n^2. && (5.3) \end{aligned}$$

Since $5n^2 - 3n + 20 \leq 25n^2$ for all $n \geq 1$, $5n^2 - 3n + 20 = O(n^2)$.

In this proof we used $c = 25$ and $n_0 = 1$.

★**Question 5.6.** Answer the following questions related to Example 5.5.

(a) What allowed us to eliminate the $-3n$ term in step 5.1? _____

_____

(b) What is the justification for step 5.2? _____

★**Evaluate 5.7.** Prove that $4n^2 - 12n + 10 = O(n^2)$.

Solution: If $n \geq 1$, $4n^2 - 12n + 10 \leq 4n^2 - 12n^2 + 10n^2 = 2n^2$. Therefore, $4n^2 - 12n + 10 = O(n^2)$.

Evaluation _____

_____

Note: *The values of the constants used in the proofs do not need to be the best possible. For instance, if you can show that $f(n) \leq 345\, g(n)$ for all $n \geq 712$, then $f(n) = O(g(n))$. It doesn't matter whether or not it is actually true that $f(n) \leq 3\, g(n)$ for all $n \geq 5$.*

★**Question 5.8.** Answer each of the following questions related to Example 5.5. Include a brief justification.

(a) Could we have used $c = 50$ in the proof?

Answer _____

_____

(b) Could we have used $c = 2$ in the proof?

Answer _____

_____

(c) Could we have used $n_0 = 100$ in the proof?

Answer _____

_____

(d) Could we have used $n_0 = 0$ in the proof?

Answer _____

_____

★**Exercise 5.9.** Prove that $5n^5-4n^4+3n^3-2n^2+n = O(n^5)$. (Hint: Use the same techniques you saw in Example 5.5.)

★**Question 5.10.** What values did you use for n_0 and c in your solution to Exercise 5.9?

$n_0 =$ _____, $c =$ _____

Things are not always so easy. How would you show that $(\sqrt{2})^{\log n} + \log^2 n + n^4 = O(2^n)$? Or that $n^2 = O(n^2 - 13n + 23)$? In general, we simply (or in some cases with much effort) find values c and n_0 that work. This gets easier with practice.

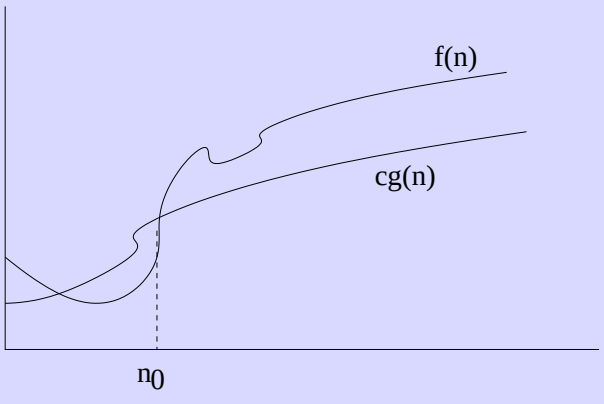
Big-O is a notation to express the idea that one function is an upper bound for another function. The next notation allows us to express the opposite idea—that one function is a *lower bound* for another function.

Definition 5.11 (Big-Omega)**.** *Let f and g be nonnegative functions.*

We say that $f(n)$ is **Big-Omega** *of $g(n)$, written as $f(n) = \Omega(g(n))$, iff there are positive constants c and n_0 such that*

$$c\,g(n) \leq f(n) \text{ for all } n \geq n_0.$$

When we say $f(n) = \Omega(g(n))$, it means that $f(n)$ grows no slower than $g(n)$. In other words, $g(n)$ is an **asymptotic lower bound** *(or just* **lower bound***) on $f(n)$.*



Example 5.12. Prove that $n^3 + 4n^2 = \Omega(n^2)$.

Proof: Here, we have $f(n) = n^3 + 4n^2$, and $g(n) = n^2$. It is not too hard to see that if $n \geq 1$,

$$n^2 \leq n^3 \leq n^3 + 4n^2$$

Therefore,

$$1n^2 \leq n^3 + 4n^2 \text{ for all } n \geq 1$$

so $n^3 + 4n^2 = \Omega(n^2)$ by definition of Ω, with $n_0 = 1$, and $c = 1$. □

★**Exercise 5.13.** Prove that $4n^2 + n + 1 = \Omega(n^2)$. (This one should be really easy—follow the technique from the previous example and don't over think it.)

★**Question 5.14.** What values did you use for n_0 and c in your solution to Exercise 5.13?

$n_0 =$ _____, $c =$ _____

Proving that $f(n) = \Omega(g(n))$ often requires more thought than proving that $f(n) = O(g(n))$. Although the lower-order terms with positive coefficients can be easily dealt with, those with negative coefficients make things a bit more complicated. Often, we have to pick $c < 1$. A good strategy is to pick a value of c that you think will work, and determine which value of n_0 is needed. Being able to do some algebra helps. As it turns out, we won't have to worry a whole lot about this, though. We will see a different technique to prove bounds shortly that, when it works, makes things much easier.

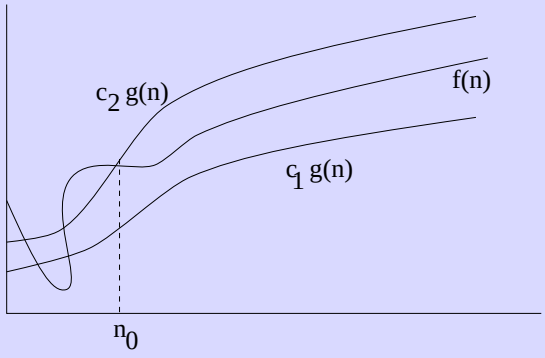
Our third notation allows us to express the idea that two functions grow at the same rate.

Definition 5.15 (Big-Theta)**.** *Let f and g be nonnegative functions.*

We say that $f(n)$ is **Big-Theta** *of $g(n)$, written as $f(n) = \Theta(g(n))$, iff there are positive constants c_1, c_2 and n_0 such that*

$$c_1\, g(n) \leq f(n) \leq c_2\, g(n) \text{ for all } n \geq n_0.$$

If $f(n) = \Theta(g(n))$, $f(n)$ grows at the same rate as $g(n)$. In other words, $g(n)$ is an **asymptotically tight bound** *(or just* **tight bound***) on $f(n)$.*



Example 5.16. Prove that $n^2 + 5n + 7 = \Theta(n^2)$

Proof: When $n \geq 1$, $n^2 + 5\,n + 7 \leq n^2 + 5\,n^2 + 7n^2 \leq 13n^2$.

When $n \geq 0$, $n^2 \leq n^2 + 5\,n + 7$.

Combining these, we can see that when $n \geq 1$,

$$n^2 \leq n^2 + 5\,n + 7 \leq 13\,n^2,$$

so $n^2+5\,n+7 = \Theta(n^2)$ by definition of Θ, with n_0=1, c_1=1, and c_2=13. □

★**Question 5.17.** In the previous example, we combined two inequalities. One of them assumed $n \geq 0$, the other assumed that $n \geq 1$. In the combined inequality, we said it held if $n \geq 1$. Is that really O.K., or did we make a subtle error?

Answer _____

_____

Using the definition of Θ can be inconvenient since it involves a double inequality. Luckily, the following theorem provides us with an easier approach.

Theorem 5.18. *If f and g are nonnegative functions, then $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.*

Proof: *The result follows almost immediately from the definitions. We leave the details to the reader.* □

This theorem implies that no new strategies are necessary for Θ proofs since they can be split into two proofs—a Big-O proof and a Ω proof. Let's see an example of this approach.

Example 5.19. Show that $\frac{1}{2}n^2 + 3\,n = \Theta(n^2)$

Proof: Notice that if $n \geq 1$,

$$\frac{1}{2}n^2 + 3\,n \leq \frac{1}{2}n^2 + 3\,n^2 = \frac{7}{2}n^2,$$

so $\frac{1}{2}n^2 + 3\,n = O(n^2)$. Also, when $n \geq 0$,

$$\frac{1}{2}n^2 \leq \frac{1}{2}n^2 + 3n,$$

so $\frac{1}{2}n^2 + 3\,n = \Omega(n^2)$. Since $\frac{1}{2}n^2 + 3\,n = O(n^2)$ and $\frac{1}{2}n^2 + 3\,n = \Omega(n^2)$, then by Theorem 5.18, $\frac{1}{2}n^2 + 3\,n = \Theta(n^2)$ □

How do you use asymptotic notation to express that $f(n)$ grows slower than $g(n)$? Saying $f(n) = O(g(n))$ doesn't work, because that only tells us that $f(n)$ grows *no faster than* $g(n)$. It

might grow slower, but it also might grow at the same rate. With the notation we have, the best way to express this idea is to say that $f(n) = O(g(n))$ and $f(n) \neq \Theta(g(n))$. But that is awkward. Let's learn a new notation for this instead. For technical reasons that we won't get into, this notation has to be defined somewhat differently than the others.

Definition 5.20. *Let f and g be nonnegative functions, with g being eventually non-zero. We say that $f(n)$ is* **little-o** *of $g(n)$, written $f(n) = o(g(n))$ iff*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

If $f(n) = o(g(n))$, $f(n)$ grows **asymptotically slower** *than $g(n)$.*

Example 5.21. You should be able to convince yourself that $3n+2 = o(n^2)$, but $3n+2 \neq o(n)$. Similarly, $n^2+n+4 = o(n^3)$ and $n^2+n+4 = o(n^4)$, but $n^2+n+4 \neq o(n^2)$ and $n^2+n+4 \neq o(n)$.

If you are not comfortable with limits you can still convince yourself of these statements by thinking of the informal definition. For instance, $n^2 + n + 4$ grows slower than n^3 so $n^2 + n + 4 = o(n^3)$. On the other hand, $n^2 + n + 4$ grows at the same rate (so *not* slower than) n^2, so $n^2 + n + 4 \neq o(n^2)$.

★**Question 5.22.** Why do we require that $g(n)$ be eventually non-zero in the definition of little-o?

Answer _____

Little-omega (ω) can be defined similarly to little-o, but the value of the limit is ∞ instead of 0. We won't use ω very often.

★**Question 5.23.** Big-O notation is analogous to $\leq$ in certain ways. If so, what would be the similar analogies for o and ω?

Answer _____

Note:

- *It is important to remember that a O-bound is only an* **upper bound***, and that it may or may not be a tight bound. So if $f(n) = O(n^2)$, it is possible that $f(n) = 3n^2 + 4$, $f(n) = \log n$, or any other function that grows no faster than n^2. But we also know that $f(n) \neq n^3$ or any other function that grows faster than n^2.*
- *Conversely, a Ω-bound is only a* **lower bound***. Thus, if $f(n) = \Omega(n \log n)$, it might be the case that $f(n) = 2^n$, but we know that $f(n) \neq 3n$, for instance.*
- *Unlike the others, Θ-bounds are precise. So, if $f(n) = \Theta(n^2)$, then we know that f has quadratic growth rate. It might be that $f(n) = 3n^2$, $2n^2 - 43n - 4$, or even $n^2 + n \log n$. But we are certain that the fastest growing term of f is cn^2 for some constant c.*

★**Question 5.24.** Answer the following questions about the asymptotic notations.

(a) If $f(n) = \Theta(g(n))$, is it possible that $f(n) = o(g(n))$? Explain.

(b) If $f(n) = O(g(n))$, is it possible that $f(n) = o(g(n))$? Explain.

(c) If $f(n) = O(g(n))$, is it *certain* that $f(n) = o(g(n))$? Explain.

(d) If $f(n) = o(g(n))$, is it possible that $f(n) = O(g(n))$? Explain.

★**Evaluate 5.25.** Let $a_0, \ldots, a_k \in \mathbb{R}$, where $a_k > 0$. Prove that $a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 = O(n^k)$.

Solution I: We can first eliminate all of the constants since they become irrelevant as n grows large enough. This leaves us with $n^k + n^{k-1} + \cdots + n = O(n^k)$. Next we can eliminate all terms growing slower than n^k, since they also become irrelevant as n grows. This leaves us with $n^k = O(n^k)$, and since they are the same, they are effectively theta of each other, and by definition, anything that is theta of something is also omega and O, so we can correctly say that $n^k = O(n^k)$, thus proving that $a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 = O(n^k)$.

Evaluation

Solution 2: Let $c = \sum_{i=0}^{k} |a_i|$. Then if $n \geq 1$,

$$\begin{aligned} a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 &\leq |a_k| n^k + |a_{k-1}| n^{k-1} + \cdots + |a_1| n + |a_0| \\ &\leq |a_k| n^k + |a_{k-1}| n^k + \cdots + |a_1| n^k + |a_0| n^k \\ &\leq \sum_{i=0}^{k} |a_i| n^k = c n^k. \end{aligned}$$

Therefore, $a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 = O(n^k)$.

Evaluation _____

_____

_____

★**Exercise 5.26.** Assume that $f(n) = O(n^2)$ and $g(n) = O(n^3)$. What can you say about the relative growth rates of $f(n)$ and $g(n)$? In particular, does $g(n)$ grow faster than $f(n)$?

Answer _____

_____

_____

Keep in mind that asymptotic notation only allows you to compare the asymptotic behavior of functions. Except for Θ-notation, it only provides a bound on the growth rate. For instance, knowing that $f(n) = O(g(n))$ only tells you that $f(n)$ grows no faster than $g(n)$. It is possible that $f(n)$ grows a lot slower than $g(n)$.

★**Exercise 5.27.** Let's test your understanding of the material so far. Answer each of the following true/false questions, giving a very brief justification/counterexample. Justifications can appeal to a definition and/or theorem. For counterexamples, use simple functions. For instance, $f(n) = n$ and $g(n) = n^2$.

(a) ___If $f(n) = O(g(n))$, then $f(n)$ grows faster than $g(n)$

(b) ___If $f(n) = \Theta(g(n))$, then $f(n)$ grows faster than $g(n)$

(c) ___If $f(n) = O(g(n))$, then $f(n)$ grows at the same rate as $g(n)$

(d) ___If $f(n) = \Omega(g(n))$, then $f(n)$ grows faster than $g(n)$

(e) ___If $f(n) = O(g(n))$, then $f(n) = \Omega(g(n))$

(f) ___If $f(n) = \Theta(g(n))$, then $f(n) = O(g(n))$

(g) ___If $f(n) = O(g(n))$, then $f(n) = \Theta(g(n))$

(h) ___If $f(n) = O(g(n))$, then $g(n) = O(f(n))$

5.1.2 Properties of the Notations

There are a lot of properties that hold for Big-O, Θ and Ω notation (and o and ω as well, but we won't focus on those ones in this section). We will only present a few of the most important ones. We provide proofs for some of the results. The rest can be proven without too much difficulty using the definitions of the notations.

Before we present the properties, it might be useful to think about the properties of things you are already familiar with. For instance, given real numbers x, y and z, you know that if $x \leq y$ and $y \leq z$, then $x \leq z$. This is just the transitive property of $\leq$. Similarly, you know that if $x \leq y$, then $a\,x \leq a\,y$ for any positive constant a. You can think of Big-O notation as being like $\leq$, Θ notation as being like $=$, and Ω notation as being like $\geq$. Many of the properties of $\leq$, $=$ and $\geq$ that you are already familiar with have an analog with Big-O, Θ, and Ω notation. But you need to be careful because the analogies are not exact. For instance, constants cannot be ignored with inequalities but can be ignored when using asymptotic notation.

Theorem 5.28. *The transitive property holds for Big-O, Θ, and Ω. That is,*

- *If $f(n) = O(g(n))$ and $g(n) = O(h(n))$, then $f(n) = O(h(n))$*
- *If $f(n) = \Theta(g(n))$ and $g(n) = \Theta(h(n))$, then $f(n) = \Theta(h(n))$*
- *If $f(n) = \Omega(g(n))$ and $g(n) = \Omega(h(n))$, then $f(n) = \Omega(h(n))$*

Proof: *You will prove the transitive property of Big-O in Exercise 5.49. The proofs of the other two are very similar.* □

Theorem 5.28 is pretty intuitive. For instance, when applied to Big-O notation, Theorem 5.28 is essentially stating that if $g(n)$ is an upper bound on $f(n)$ and $h(n)$ is an upper bound on $g(n)$, then $h(n)$ is an upper bound for $f(n)$. Put another way, if $f(n)$ grows no faster than $g(n)$ and $g(n)$

grows no faster than $h(n)$, then $f(n)$ grows no faster than $h(n)$. This makes perfect sense if you think about it for a few minutes.

Example 5.29. Let's take it for granted that $4n^2 + 3n + 17 = O(n^3)$ and $n^3 = O(n^4)$ (both of which you should be able to easily prove at this point). According to Theorem 5.28, we can conclude that $4n^2 + 3n + 17 = O(n^4)$.

Theorem 5.30. *Scaling by a constant factor*
If $f(n) = O(g(n))$, then for any $k > 0$, $kf(n) = O(g(n))$. Similarly for Θ and Ω.

> **Proof:** *We will give the proof for Big-O notation. The other two proofs are similar. Assume $f(n) = O(g(n))$. Then by the definition of Big-O, there are positive constants c and n_0 such that $f(n) \leq c\,g(n)$ for all $n \geq n_0$. Thus, if $n \geq n_0$,*
>
> $$k\,f(n) \leq k\,c\,g(n) = c'g(n),$$
>
> *where $c' = k\,c$ is a positive constant. By the definition of Big-O, $kf(n) = O(g(n))$.* □

Example 5.31. Example 5.19 showed that $\frac{1}{2}n^2 + 3\,n = \Theta(n^2)$. We can use Theorem 5.30 to conclude that $n^2 + 6\,n = \Theta(n^2)$ since $n^2 + 6\,n = 2\left(\frac{1}{2}n^2 + 3\,n\right)$.

Perhaps now is a good time to point out a related issue. Typically, we do not include constants inside asymptotic notations. For instance, although it is technically correct to say that $34n^3 + 2n^2 - 45n + 5 = O(5n^3)$ (or $O(50n^3)$, or any other constant you care to place there), it is best to just say it is $O(n^3)$. In particular, $\Theta(1)$ may be preferable to $\Theta(k)$.

Theorem 5.32. *Sums*
If $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then

$$f_1(n) + f_2(n) = O(g_1(n) + g_2(n)) = O(max\{g_1(n), g_2(n)\}).$$

Similarly for Θ and Ω.

> **Proof:** *We will prove the assertion for Big-O. Assume $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$. Then there exists positive constants c_1 and n_1 such that for all $n \geq n_1$,*
>
> $$f_1(n) \leq c_1 g_1(n),$$
>
> *and there exists positive constants c_2 and n_2 such that for all $n \geq n_2$,*
>
> $$f_2(n) \leq c_2 g_2(n).$$
>
> *Let $c_0 = \max\{c_1, c_2\}$ and $n_0 = \max\{n_1, n_2\}$. Since n_0 is at least as large as n_1 and n_2, then for all $n \geq n_0$, $f_1(n) \leq c_1 g_1(n)$ and $f_2(n) \leq c_2 g_2(n)$. (If you don't see why this is, think about it. This is a subtle but important step.) Similarly, if $f_1(n) \leq c_1 g_1(n)$, then clearly $f_1(n) \leq c_0 g_1(n)$ since c_0 is at least as big as c_1 (and*

similarly for f_2). Then for all $n \geq n_0$, we have

$$\begin{aligned} f_1(n) + f_2(n) &\leq c_1 g_1(n) + c_2 g_2(n) \\ &\leq c_0 g_1(n) + c_0 g_2(n) \\ &\leq c_0[g_1(n) + g_2(n)] \\ &\leq c_0[\max\{g_1(n), g_2(n)\} + \max\{g_1(n), g_2(n)\}] \\ &\leq 2c_0 \max\{g_1(n), g_2(n)\} \\ &\leq c \max\{g_1(n), g_2(n)\}, \end{aligned}$$

where $c = 2c_0$. By the definition of Big-O, we have shown that $f_1(n) + f_2(n) = O(max\{g_1(n), g_2(n)\})$. □

Notice that in this proof we used $c = 2\max\{c_1, c_2\}$ and $n_0 = \max\{n_1, n_2\}$.

Without getting too technical, the previous theorem implies that you can upper bound the sum of two or more functions by finding the upper bound of the fastest growing of the functions. Another way of thinking about it is if you ever have two or more functions inside Big-O notation, you can simplify the notation by omitting the slower growing function(s). It should be pointed out that there is a subtle point in this result about how to precisely define the maximum of two functions. Most of the time the intuitive definition is sufficient so we won't belabor the point.

Example 5.33. Since we have previously shown that $5n^2-3n+20 = O(n^2)$ and that $3n^3-2n^2+13n-15 = O(n^3)$, we know that $(5n^2-3n+20)+(3n^3-2n^2+13n-15) = O(n^2+n^3) = O(n^3)$.

Theorem 5.34. *Products*
If $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then

$$f_1(n)f_2(n) = O(g_1(n)g_2(n)).$$

Similarly for Θ and Ω.

Example 5.35. Since we have previously shown that $5n^2 - 3n + 20 = O(n^2)$ and that $3n^3 - 2n^2+13n-15 = O(n^3)$, we know that $(5n^2-3n+20)(3n^3-2n^2+13n-15) = O(n^2n^3) = O(n^5)$. Notice that we could arrive at this same conclusion by multiplying the two polynomials and taking the highest term. However, this would require a lot more work than is necessary.

The next theorem essentially says that if $g(n)$ is an upper bound on $f(n)$, then $f(n)$ is a lower bound on $g(n)$. This makes perfect sense if you think about it.

Theorem 5.36. *Symmetry (sort of)*
$f(n) = O(g(n))$ iff $g(n) = \Omega(f(n))$.

It turns out that Θ defines an equivalence relation on the set of functions from $\mathbf{Z}^+$ to $\mathbf{Z}^+$. That is, it defines a partition on these functions, with two functions being in the same partition (or the same equivalence class) if and only if they have the same growth rate. But don't take our word for it. You will help to prove this fact next.

★**Fill in the details 5.37.** Let R be the relation on the set of functions from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ such that $(f, g) \in R$ if and only if $f = \Theta(g)$. Show that R is an equivalence relation.

Proof: We need to show that R is reflexive, symmetric, and transitive.

Reflexive: Since $1 \cdot f(n) \leq f(n) \leq 1 \cdot f(n)$ for all $n \geq 1$, $f(n) = \Theta(f(n))$, so R is reflexive.

Symmetric: If $f(n) = \Theta(g(n))$, then there exist positive constants c_1, c_2, and n_0 such that _____

This implies that

$$g(n) \leq \frac{1}{c_1} f(n) \text{ and } g(n) \geq \frac{1}{c_2} f(n) \text{ for all } n \geq n_0$$

which is equivalent to

_____ $\leq g(n) \leq$ _____ for all $n \geq n_0$.

Thus $g(n) = \Theta(f(n))$, and R is symmetric.

Transitive: If $f(n) = \Theta(g(n))$, then there exist positive constants c_1, c_2, and n_0 such that

$$c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for all } n \geq n_0.$$

Similarly if $g(n) = \Theta(h(n))$, then there exist positive constants c_3, c_4, and n_1 such that _____

Then

$$f(n) \geq c_1\, g(n) \geq c_1 c_3\, h(n) \text{ for all } n \geq \max\{n_0, n_1\},$$

and

$f(n) \leq$ _____ $g(n) \leq$ _____ $h(n)$ for all $n \geq$ _____

Thus, _____ $\leq f(n) \leq$ _____ for all $n \geq \max\{n_0, n_1\}$.

Since $c_1 c_3$ and $c_2 c_4$ are both positive constants, $f(n) =$ _____ by the definition of _____, so R is _____. □

Example 5.38. The functions n^2, $3n^2 - 4n + 4$, $n^2 + \log n$, and $3n^2 + n + 1$ are all $\Theta(n^2)$. That is, they all have the same rate of growth and all belong to the same equivalence class.

★**Exercise 5.39.** Let's test your understanding of the material so far. Answer each of the following true/false questions, giving a very brief justification/counterexample. Justifications can appeal to a definition and/or theorem. For counterexamples, use simple functions. For instance, $f(n) = n$ and $g(n) = n^2$.

(a) ___If $f(n) = O(g(n))$, then $g(n) = \Omega(f(n))$

(b) ___If $f(n) = \Theta(g(n))$, then $f(n) = \Omega(g(n))$ and $f(n) = O(g(n))$

(c) ___If $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then $f_1(n) + f_2(n) = O(max(g_1(n), g_2(n)))$

(d) ___$f(n) = O(g(n))$ iff $f(n) = \Theta(g(n))$

(e) ___$f(n) = O(g(n))$ iff $g(n) = O(f(n))$

(f) ___$f(n) = O(g(n))$ iff $g(n) = \Omega(f(n))$

(g) ___$f(n) = \Theta(g(n))$ iff $f(n) = \Omega(g(n))$ and $f(n) = O(g(n))$

(h) ___If $f(n) = O(g(n))$ and $g(n) = O(h(n))$, then $f(n) = O(h(n))$

5.1.3 Proofs using the definitions

In this section we provide more examples and exercises that use the definitions to prove bounds.

The first example is annotated with comments (given in footnotes) about the techniques that are used in many of these proofs. We use the following terminology in our explanation. By *lower order term* we mean a term that grows slower, and *higher order* means a term that grows faster. The *dominating term* is the term that grows the fastest. For instance, in $x^3 + 7\,x^2 - 4$, the x^2 term is a lower order term than x^3, and x^3 is the dominating term. We will discuss common growth rates, including how they relate to each other, in Section 5.2. But for now we assume you know that x^5 grows faster than x^3, for instance.

Example 5.40. Find a tight bound on $f(n) = n^8 + 7n^7 - 10n^5 - 2n^4 + 3n^2 - 17$.

Solution: We will prove that $f(n) = \Theta(n^8)$. First, we will prove an upper bound for $f(n)$. It is clear that when $n \geq 1$,

$$\begin{aligned} n^8 + 7n^7 - 10n^5 - 2n^4 + 3n^2 - 17 &\leq n^8 + 7n^7 + 3n^2 \quad [a] \\ &\leq n^8 + 7n^8 + 3n^8 \quad [b] \\ &= 11n^8 \end{aligned}$$

Thus, we have

$$f(n) = n^8 + 7n^7 - 10n^5 - 2n^4 + 3n^2 - 17 \leq 11n^8 \text{ for all } n \geq 1,$$

and we have proved that $f(n) = O(n^8)$.

Now, we will prove the lower bound for $f(n)$. When $n \geq 1$,

$$\begin{aligned} n^8 + 7n^7 - 10n^5 - 2n^4 + 3n^2 - 17 &\geq n^8 - 10n^5 - 2n^4 - 17 \quad [c] \\ &\geq n^8 - 10n^7 - 2n^7 - 17n^7 \quad [d] \\ &= n^8 - 29n^7 \end{aligned}$$

Next, we need to find a value $c > 0$ such that $n^8 - 29n^7 \geq cn^8$. Doing a little algebra, we see that this is equivalent to $(1 - c)n^8 \geq 29n^7$. When $n \geq 1$, we can divide by n^7 and obtain $(1 - c)n \geq 29$. Solving for c we obtain

$$c \leq 1 - \frac{29}{n}.$$

If $n \geq 58$, then $c = 1/2$ suffices. We have just shown that if $n \geq 58$, then

$$f(n) = n^8 + 7n^7 - 10n^5 - 2n^4 + 3n^2 - 17 \geq \frac{1}{2}n^8.$$

Thus, $f(n) = \Omega(n^8)$. Since we have shown that $f(n) = \Omega(n^8)$ and that $f(n) = O(n^8)$, we have shown that $f(n) = \Theta(n^8)$.

[a] We can upper bound any function by removing the lower order terms with negative coefficients, as long as $n \geq 0$.

[b] We can upper bound any function by replacing lower order terms that have positive coefficients by the dominating term with the same coefficients. Here, we must make sure that the dominating term is larger than the given term for all values of n larger than some threshold n_0, and we must make note of the threshold value n_0.

[c] We can lower bound any function by removing the lower order terms with positive coefficients, as long as $n \geq 0$.

[d] We can lower bound any function by replacing lower order terms with negative coefficients by a sub-dominating term with the same coefficients. (By sub-dominating, I mean one which dominates all but the dominating term.) Here, we must make sure that the sub-dominating term is larger than the given term for all values of n larger than some threshold n_0, and we must make note of the threshold value n_0. Making a wise choice for which sub-dominating term to use is crucial in finishing the proof.

Let's see another example of a Ω proof. You should note the similarities between this and the second half of the proof in the previous example.

Example 5.41. Show that $(n \log n - 2n + 13) = \Omega(n \log n)$

Proof: We need to show that there exist positive constants c and n_0 such that

$$c\, n \log n \leq n \log n - 2n + 13 \text{ for all } n \geq n_0.$$

Since $n \log n - 2n \leq n \log n - 2n + 13$, we will instead show that

$$c\, n \log n \leq n \log n - 2n,$$

which is equivalent to

$$c \leq 1 - \frac{2}{\log n}, \text{ when } n > 1.$$

If $n \geq 8$, then $2/(\log n) \leq 2/3$, and picking $c = 1/3$ suffices. In other words, we have just shown that if $n \geq 8$,

$$\frac{1}{3} n \log n \leq n \log n - 2n.$$

Thus if $c = 1/3$ and $n_0 = 8$, then for all $n \geq n_0$, we have

$$c\, n \log n \leq n \log n - 2n \leq n \log n - 2n + 13.$$

Thus $(n \log n - 2n + 13) = \Omega(n \log n)$. □

★**Fill in the details 5.42.** Show that $\frac{1}{2}n^2 - 3n = \Theta(n^2)$

Proof: We need to find positive constants c_1, c_2, and n_0 such that

$$\_\_\_\_\_ \leq \frac{1}{2}n^2 - 3n \leq \_\_\_\_\_ \text{ for all } n \geq n_0$$

Dividing by n^2, we get $c_1 \leq$ _____ $\leq c_2$.

Notice that if $n \geq 10$, $\frac{1}{2} - \frac{3}{n} \geq \frac{1}{2} - \frac{3}{10} =$ _____, so we can choose $c_1 = 1/5$. If $n \geq 10$, we also have that $\frac{1}{2} - \frac{3}{n} \leq \frac{1}{2}$, so we can choose $c_2 = 1/2$. Thus, we have shown that

$$\_\_\_\_\_ \leq \frac{1}{2}n^2 - 3n \leq \_\_\_\_\_ \text{ for all } n \geq \_\_\_\_\_.$$

Therefore, $\frac{1}{2}n^2 - 3n = \Theta(n^2)$. □

★**Question 5.43.** In the previous proof, we claimed that if $n \geq 10$,

$$\frac{1}{2} - \frac{3}{n} \geq \frac{1}{2} - \frac{3}{10}.$$

Why is this true?

Answer _____

_____

_____

Example 5.44. Show that $(\sqrt{2})^{\log n} = O(\sqrt{n})$, where the base of the log is 2.

Proof: It is not too hard to see that

$$(\sqrt{2})^{\log n} = n^{\log \sqrt{2}} = n^{\log 2^{1/2}} = n^{\frac{1}{2}\log 2} = n^{\frac{1}{2}} = \sqrt{n}.$$

Thus it is clear that $(\sqrt{2})^{\log n} = O(\sqrt{n})$. □

Note: *You may be confused by the previous proof. It seems that we never showed that* $(\sqrt{2})^{\log n} \leq c\sqrt{n}$ *for some constant* c*. But we essentially did by showing that* $(\sqrt{2})^{\log n} = \sqrt{n}$ *since this implies that* $(\sqrt{2})^{\log n} \leq 1\sqrt{n}$*.*

We actually proved something stronger than was required. That is, since we proved the two functions are equal, it is in fact true that $(\sqrt{2})^{\log n} = \Theta(\sqrt{n})$*. But we were only asked to prove that* $(\sqrt{2})^{\log n} = O(\sqrt{n})$*.*

In general, if you need to prove a Big-O bound, you may instead prove a Θ *bound, and the Big-O bound essentially comes along for the ride.*

★**Question 5.45.** In our previous note we mentioned that if you prove a Θ bound, you get the Big-O bound for free.

(a) What theorem implies this?

Answer _____

(b) If we prove $f(n) = O(g(n))$, does that imply that $f(n) = \Theta(g(n))$? In other words, does it work the other way around? Explain, giving an appropriate example.

Answer _____

_____

★**Exercise 5.46.** Show that $n! = O(n^n)$. (Don't give up too easily on this one—the proof is very short and only uses elementary algebra.)

Example 5.47. Show that $\log(n!) = O(n \log n)$

Proof: It should be clear that if $n \geq 1$, $n! \leq n^n$ (especially after completing the previous exercise). Taking logs of both sides of that inequality, we obtain

$$\log n! \leq \log(n^n) = n \log n.$$

Therefore $\log n! = O(n \log n)$. □

The last step used the fact that $\log(f(n)^a) = a \log(f(n))$, a fact that we assume you have seen previously (but may have forgotten).

Proving properties of the asymptotic notations is actually no more difficult than the rest of the proofs we have seen. You have already seen a few and helped write one. Here we provide one more example and then ask you to prove another result on your own.

Example 5.48. Prove that if $f(n) = O(g(n))$ and $g(n) = O(f(n))$, then $f(n) = \Theta(g(n))$.

Proof: If $f(n) = O(g(n))$, then there are positive constants c_2 and n_0' such that

$$f(n) \leq c_2\, g(n) \text{ for all } n \geq n_0'$$

Similarly, if $g(x) = O(f(x))$, then there are positive constants c_1' and n_0'' such that

$$g(n) \leq c_1'\, f(n) \text{ for all } n \geq n_0''.$$

We can divide this by c_1' to obtain

$$\frac{1}{c_1'} g(n) \leq f(n) \text{ for all } n \geq n_0''.$$

Setting $c_1 = 1/c_1'$ and $n_0 = \max\{n_0', n_0''\}$, we have

$$c_1 g(n) \leq f(n) \leq c_2\, g(n) \text{ for all } n \geq n_0.$$

Thus, $f(x) = \Theta(g(x))$. □

★**Exercise 5.49.** Let $f(x) = O(g(x))$ and $g(x) = O(h(x))$. Show that $f(x) = O(h(x))$. That is, prove Theorem 5.28 for Big-O notation.

5.1.4 Proofs using limits

So far we have used the definitions of the various notations in all of our proofs. The following theorem provides another technique that is often much easier, assuming you understand and are comfortable with limits.

Theorem 5.50. *Let $f(n)$ and $g(n)$ be functions such that*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = A.$$

Then

1. *If $A = 0$, then $f(n) = O(g(n))$, and $f(n) \neq \Theta(g(n))$. That is, $f(n) = o(g(n))$.*
2. *If $A = \infty$, then $f(n) = \Omega(g(n))$, and $f(n) \neq \Theta(g(n))$. That is, $f(n) = \omega(g(n))$.*
3. *If $A \neq 0$ is finite, then $f(n) = \Theta(g(n))$.*

If the above limit does not exist, then you need to resort to using the definitions or using some other technique. Luckily, the above approach works most of the time.

Before we see some examples, let's review a few limits you should know.

Theorem 5.51. *Let a and c be real numbers. Then*

(a) $\lim_{n\to\infty} a = a$

(b) If $a > 0$, $\lim_{n\to\infty} n^a = \infty$

(c) If $a < 0$, $\lim_{n\to\infty} n^a = 0$

(d) If $a > 1$, $\lim_{n\to\infty} a^n = \infty$

(e) If $0 < a < 1$, $\lim_{n\to\infty} a^n = 0$

(f) If $c > 0$, $\lim_{n\to\infty} \log_c n = \infty$.

Example 5.52. The following are examples based on Theorem 5.51.

(a) $\lim_{n\to\infty} 13 = 13$

(b) $\lim_{n\to\infty} n = \infty$

(c) $\lim_{n\to\infty} n^4 = \infty$

(d) $\lim_{n\to\infty} n^{1/2} = \infty$

(e) $\lim_{n\to\infty} n^{-2} = 0$

(f) $\lim_{n\to\infty} \left(\frac{1}{2}\right)^n = 0$

(g) $\lim_{n\to\infty} 2^n = \infty$

(h) $\lim_{n\to\infty} \log_2 n = \infty$

Now it's your turn to try a few.

★**Exercise 5.53.** Evaluate the following limits

(a) $\lim_{n\to\infty} \log_{10} n =$

(b) $\lim_{n\to\infty} n^3 =$

(c) $\lim_{n\to\infty} 3^n =$

(d) $\lim_{n\to\infty} \left(\frac{3}{2}\right)^n =$

(e) $\lim_{n\to\infty} \left(\frac{2}{3}\right)^n =$

(f) $\lim_{n\to\infty} n^{-1} =$

(g) $\lim_{n\to\infty} 8675309 =$

Example 5.54. Prove that $5n^8 = \Theta(n^8)$ using Theorem 5.50.

Solution: Notice that

$$\lim_{n\to\infty} \frac{5n^8}{n^8} = \lim_{n\to\infty} 5 = 5,$$

so $f(n) = \Theta(n^8)$ by Theorem 5.50 (case 3).

The following theorem often comes in handy when using Theorem 5.50.

Theorem 5.55. *If* $\lim_{n\to\infty} f(n) = \infty$, *then* $\lim_{n\to\infty} \frac{1}{f(n)} = 0$.

Example 5.56. Prove that $n^2 = o(n^4)$ using Theorem 5.50.

Solution: Notice that

$$\lim_{n\to\infty} \frac{n^2}{n^4} = \lim_{n\to\infty} \frac{1}{n^2} = 0,$$

so $f(n) = o(n^4)$ by Theorem 5.50 (case 1).

★**Question 5.57.** The proof in the previous example used Theorems 5.51 and 5.55. How and where?

Answer _____

_____

★**Exercise 5.58.** Prove that $3x^3 = \Omega(x^2)$ using Theorem 5.50. Which case did you use?

Here are a few more useful properties of limits. Read carefully. These do not apply in all situations.

Theorem 5.59. *Let a be a finite real number and let $\lim_{n\to\infty} f(n) = A$ and $\lim_{n\to\infty} g(n) = B$, where A and B are finite real numbers. Then*

(a) $\lim_{n\to\infty} a\, f(n) = a\, A$

(b) $\lim_{n\to\infty} f(n) \pm g(n) = A \pm B$

(c) $\lim_{n\to\infty} f(n)g(n) = AB$

(d) If $B \neq 0$, $\lim_{n\to\infty} \dfrac{f(n)}{g(n)} = \dfrac{A}{B}$

We usually use the results from the previous theorem without explicitly mentioning them.

Example 5.60. Find a tight bound on $f(x) = x^8 + 7x^7 - 10x^5 - 2x^4 + 3x^2 - 17$ using Theorem 5.50.

Solution: We guess (or know, if we remember the solution to Example 5.40) that $f(x) = \Theta(x^8)$. To prove this, notice that

$$\begin{aligned}
\lim_{x\to\infty} x^8+7x^7-10x^5-2x^4+3x^2-\frac{17}{x^8} &= \lim_{x\to\infty} \frac{x^8}{x^8} + \frac{7x^7}{x^8} - \frac{10x^5}{x^8} - \frac{2x^4}{x^8} + \frac{3x^2}{x^8} - \frac{17}{x^8} \\
&= \lim_{x\to\infty} 1 + \frac{7}{x} - \frac{10}{x^3} - \frac{2}{x^4} + \frac{3}{x^6} - \frac{17}{x^8} \\
&= 1 + 0 - 0 - 0 + 0 - 0 = 1
\end{aligned}$$

Thus, $f(x) = \Theta(x^8)$ by the Theorem 5.50.

Compare the proof above with the proof given in Example 5.40. It should be pretty obvious that using Theorem 5.50 makes the proof a lot easier. Let's see another example that lets us compare the two proof methods.

Example 5.61. Prove that $f(x) = x^4 - 23x^3 + 12x^2 + 15x - 21 = \Theta(x^4)$.

Proof #1

We will use the definition of Θ. It is clear that when $x \geq 1$,

$$x^4 - 23x^3 + 12x^2 + 15x - 21 \leq x^4 + 12x^2 + 15x \leq x^4 + 12x^4 + 15x^4 = 28x^4.$$

Also, if $x \geq 88$, then $\frac{1}{2}x^4 \geq 44x^3$ or $-44x^3 \geq -\frac{1}{2}x^4$, so we have that

$$x^4 - 23x^3 + 12x^2 + 15x - 21 \geq x^4 - 23x^3 - 21 \geq x^4 - 23x^3 - 21x^3 = x^4 - 44x^3 \geq \frac{1}{2}x^4.$$

Thus

$$\frac{1}{2}x^4 \leq x^4 - 23x^3 + 12x^2 + 15x - 21 \leq 28x^4, \text{ for all } x \geq 88.$$

We have shown that $f(x) = x^4 - 23x^3 + 12x^2 + 15x - 21 = \Theta(x^4)$. □

If you did not follow the steps in this first proof, you should really review your algebra rules.

Proof #2

Since

$$\begin{aligned} \lim_{x\to\infty} \frac{x^4 - 23x^3 + 12x^2 + 15x - 21}{x^4} &= \lim_{x\to\infty} \frac{x^4}{x^4} - \frac{23x^3}{x^4} + \frac{12x^2}{x^4} + \frac{15x}{x^4} - \frac{21}{x^4} \\ &= \lim_{x\to\infty} 1 - \frac{23}{x} + \frac{12}{x^2} + \frac{15}{x^3} - \frac{21}{x^4} \\ &= \lim_{x\to\infty} 1 - 0 + 0 + 0 - 0 = 1, \end{aligned}$$

$f(x) = x^4 - 23x^3 + 12x^2 + 15x - 21 = \Theta(x^4)$ □

Example 5.62. Prove that $n(n+1)/2 = O(n^3)$ using Theorem 5.50.

Proof: Because $\lim_{n\to\infty} \frac{n(n+1)/2}{n^3} = \lim_{n\to\infty} \frac{n^2+n}{2n^3} = \lim_{n\to\infty} \frac{1}{2n} + \frac{1}{2n^2} = 0 + 0 = 0$, $n(n+1)/2 = o(n^3)$, which implies that $n(n+1)/2 = O(n^3)$. □

★**Exercise 5.63.** Prove that $n(n+1)/2 = \Theta(n^2)$ using Theorem 5.50.

★**Exercise 5.64.** Prove that $2^x = O(3^x)$

(a) Using Theorem 5.50.

(b) Using the definition of Big-O.

Now is probably a good time to recall a very useful theorem for computing limits, called **l'Hopital's Rule**. The version presented here is restricted to limits where the variable approaches infinity since those are the only limits of interest in our context.

Theorem 5.65 (l'Hopital's Rule)**.** *Let $f(x)$ and $g(x)$ be differentiable functions. If*

$$\lim_{x\to\infty} f(x) = \lim_{x\to\infty} g(x) = 0 \text{ or}$$

$$\lim_{x\to\infty} f(x) = \lim_{x\to\infty} g(x) = \infty,$$

then

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = \lim_{x\to\infty} \frac{f'(x)}{g'(x)}$$

Example 5.66. Since $\lim_{x\to\infty} 3x = \infty$ and $\lim_{x\to\infty} x^2 = \infty$,

$$\begin{aligned}
\lim_{x\to\infty} \frac{3x}{x^2} &= \lim_{x\to\infty} \frac{3}{2x} \quad \text{(l'Hopital)} \\
&= \frac{3}{2} \lim_{x\to\infty} \frac{1}{x} \\
&= \frac{3}{2} 0 \\
&= 0.
\end{aligned}$$

Example 5.67. Since $\lim_{x\to\infty} 3x^2+4x-9=\infty$ and $\lim_{x\to\infty} 12x=\infty$,

$$\begin{aligned}\lim_{x\to\infty}\frac{3x^2+4x-9}{12x} &= \lim_{x\to\infty}\frac{6x+4}{12} \quad \text{(l'Hopital)}\\ &= \lim_{x\to\infty}\frac{1}{2}x+\frac{1}{3}\\ &= \infty\end{aligned}$$

Now let's apply it to proving asymptotic bounds.

Example 5.68. Show that $\log x = O(x)$.

Proof: Notice that

$$\begin{aligned}\lim_{x\to\infty}\frac{\log x}{x} &= \lim_{x\to\infty}\frac{\frac{1}{x}}{1} \quad \text{(l'Hopital)}\\ &= \lim_{x\to\infty}\frac{1}{x}=0.\end{aligned}$$

Therefore, $\log x = O(x)$. □

We should mention that applying l'Hopital's Rule in the first step is legal since

$$\lim_{x\to\infty}\log x=\lim_{x\to\infty}x=\infty.$$

Example 5.69. Prove that $x^3=O(2^x)$.

Proof: Notice that

$$\begin{aligned}\lim_{x\to\infty}\frac{x^3}{2^x} &= \lim_{x\to\infty}\frac{3x^2}{2^x\ln(2)} \quad \text{(l'Hopital)}\\ &= \lim_{x\to\infty}\frac{6x}{2^x\ln^2(2)} \quad \text{(l'Hopital)}\\ &= \lim_{x\to\infty}\frac{6}{2^x\ln^3(2)} \quad \text{(l'Hopital)}\\ &= 0.\end{aligned}$$

Therefore, $x^3=O(2^x)$.

As in the previous example, at each step we checked that the functions on both the top and bottom go to infinity as n goes to infinity before applying l'Hopital's Rule. Notice that we did not apply it in the final step since 6 does not go to infinity. □

★**Evaluate 5.70.** Prove that 7^x is an upper bound for 5^x, but that it is not a tight bound.

Proof 1: This is true if and only if 7^x always grows faster than 5^x which means $7^x - 5^x > 0$ for all $x \neq 0$. If it is a tight bound, then $7^x - 5^x = 0$, which is only true for $x = 0$. So 7^x is an upper bound on 5^x, but not a tight bound.

Evaluation _____

_____

Proof 2: $\lim_{x\to\infty} \frac{5^x}{7^x} = \lim_{x\to\infty} \frac{x \log 5}{x \log 7}$. Both go to infinity, but $x \log 7$ gets there faster, showing that $5^x = O(7^x)$.

Evaluation _____

_____

Proof 3: $\lim_{x\to\infty} \frac{7^x}{5^x} = \lim_{x\to\infty} \left(\frac{7}{5}\right)^x = \infty$ since $7/5 > 1$. Thus $5^x = O(7^x)$ by the limit theorem.

Evaluation _____

_____

We should mention that it is important to remember to verify that l'Hopital's Rule applies before just blindly taking derivatives. You can actually get the incorrect answer if you apply it when it should not be applied.

Example 5.71. Find and prove a simple tight bound for $\sqrt{5n^2 - 4n + 12}$.

Solution: We will show that $\sqrt{5n^2 - 4n + 12} = \Theta(n)$. Since we are letting n go to infinity, we can assume that $n > 0$. In this case, $n = \sqrt{n^2}$. Using this, we can see that

$$\lim_{n\to\infty} \frac{\sqrt{5n^2 - 4n + 12}}{n} = \lim_{n\to\infty} \sqrt{\frac{5n^2 - 4n + 12}{n^2}} = \lim_{n\to\infty} \sqrt{5 - \frac{4}{n} + \frac{12}{n^2}} = \sqrt{5}.$$

Therefore, $\sqrt{5n^2 - 4n + 12} = \Theta(n)$.

★**Exercise 5.72.** Find and prove a good simple upper bound on $n \ln(n^2 + 1) + n^2 \ln n$.

(a) Using the definition of Big-O.

(b) Using Theorem 5.50. You will probably need to use l'Hopital's Rule a few times.

Example 5.73. Find and prove a simple tight bound for $n\log(n^2) + (n-1)^2\log(n/2)$.

Solution: First notice that

$$n\log(n^2) + (n-1)^2\log(n/2) = 2n\log n + (n-1)^2(\log n - \log 2).$$

We can see that this is $\Theta(n^2 \log n)$ since

$$\begin{aligned}
\lim_{n\to\infty} \frac{n\log(n^2) + (n-1)^2\log(n/2)}{n^2\log n} &= \lim_{n\to\infty} \frac{2n\log n + (n-1)^2(\log n - \log 2)}{n^2\log n} \\
&= \lim_{n\to\infty} \frac{2}{n} + \frac{(n-1)^2}{n^2}\frac{(\log n - \log 2)}{\log n} \\
&= \lim_{n\to\infty} \frac{2}{n} + \left(1 - \frac{1}{n}\right)^2\left(1 - \frac{\log 2}{\log n}\right) \\
&= 0 + (1-0)^2(1-0) = 1.
\end{aligned}$$

★**Exercise 5.74.** Find and prove a simple tight bound for $(n^2-1)^5$. You may use either the formal definition of Θ or Theorem 5.50. (The solution uses Theorem 5.50.)

★**Exercise 5.75.** Find and prove a simple tight bound for $2^{n+1} + 5^{n-1}$. You may use either the formal definition of Θ or Theorem 5.50. (The solution uses Theorem 5.50.)

5.2 Common Growth Rates

In this section we will take a look at the relative growth rates of various functions.

Figure 5.1 shows the value of several functions for various values of n to give you an idea of their relative rates of growth. The bottom of the table is labeled relative to the last column so you can get a sense of how slow $\log_2 m$ and $\log_2(\log_2 m)$ grow. For instance, the final row is showing that $\log_2(262144) = 18$ and $\log_2(\log_2(262144)) = 4.170$.

Figures 5.2 and 5.3 demonstrate that as n increases, the constants and lower-order terms do not matter. For instance, notice that although $100n$ is much larger than 2^n for small values of n, as n increases, 2^n quickly gets much larger than $100n$. Similarly, in Figure 5.3, notice that when $n = 74$, n^3 and $n^3 + 234$ are virtually the same.

$\log_2 n$	n	$n \ln n$	n^2	n^3	2^n
0.000	1	0	1	1	2
1.000	2	1.39	4	8	4
1.585	3	3.30	9	27	8
2.000	4	5.55	16	64	16
2.321	5	8.05	25	125	32
2.585	6	10.75	36	216	64
2.807	7	13.62	49	343	128
3.000	8	16.64	64	512	256
3.170	9	19.78	81	729	512
3.321	10	23.03	100	1000	1024
3.460	11	26.38	121	1331	2048
3.585	12	29.82	144	1728	4096
3.700	13	33.34	169	2197	8192
3.807	14	36.95	196	2744	16384
3.907	15	40.62	225	3375	32768
4.000	16	44.36	256	4096	65536
4.087	17	48.16	289	4913	131072
4.170	18	52.03	324	5832	262144
$\log_2 \log_2 m$	$\log_2 m$				m

Figure 5.1: A comparison of growth rates

n	$100n$	n^2	$11n^2$	n^3	2^n
1	100	1	11	1	2
2	200	4	44	8	4
3	300	9	99	27	8
4	400	16	176	64	16
5	500	25	275	125	32
6	600	36	396	216	64
7	700	49	539	343	128
8	800	64	704	512	256
9	900	81	891	729	512
10	1000	100	1100	1000	1024
11	1100	121	1331	1331	2048
12	1200	144	1584	1728	4096
13	1300	169	1859	2197	8192
14	1400	196	2156	2744	16384
15	1500	225	2475	3375	32768
16	1600	256	2816	4096	65536
17	1700	289	3179	4913	131072
18	1800	324	3564	5832	262144
19	1900	361	3971	6859	524288

Figure 5.2: Constants don't matter

n	n^2	$n^2 - n$	$n^2 + 99$	n^3	$n^3 + 234$
2	4	2	103	8	242
6	36	30	135	216	450
10	100	90	199	1000	1234
14	196	182	295	2744	2978
18	324	306	423	5832	6066
22	484	462	583	10648	10882
26	676	650	775	17576	17810
30	900	870	999	27000	27234
34	1156	1122	1255	39304	39538
38	1444	1406	1543	54872	55106
42	1764	1722	1863	74088	74322
46	2116	2070	2215	97336	97570
50	2500	2450	2599	125000	125234
54	2916	2862	3015	157464	157698
58	3364	3306	3463	195112	195346
62	3844	3782	3943	238328	238562
66	4356	4290	4455	287496	287730
70	4900	4830	4999	343000	343234
74	5476	5402	5575	405224	405458

Figure 5.3: Lower-order terms don't matter

Figures 5.4 through 5.8 give a graphical representation of relative growth rates of functions. In these diagrams, `**` means exponentiation. For instance, `x**2` means x^2.

It is important to point out that you should *never* rely on the graphs of functions to determine relative growth rates. That is the point of Figures 5.6 and 5.7. Although graphs sometimes give

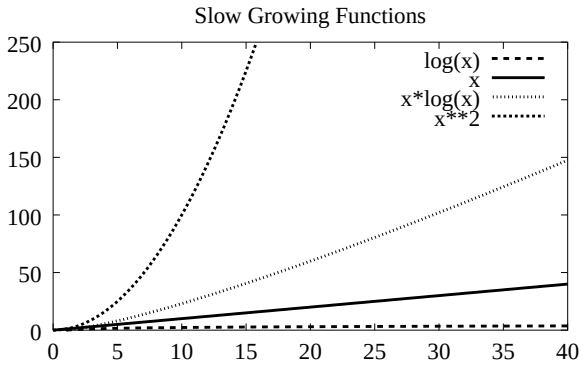


Figure 5.4: Slow growing functions.

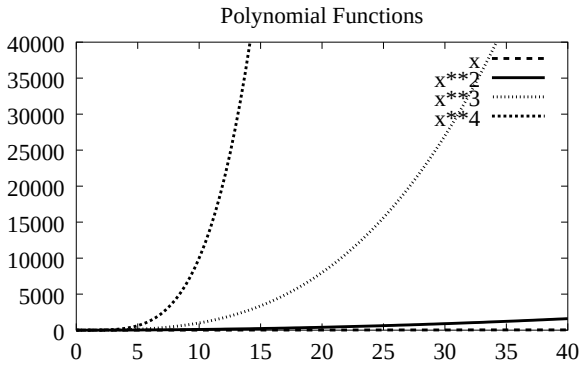


Figure 5.5: Polynomials.

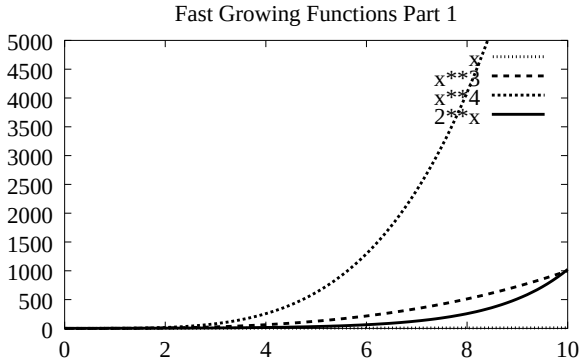


Figure 5.6: Polynomials and an exponential. It looks like x^4 grows faster than 2^x, but see Fig 5.7.

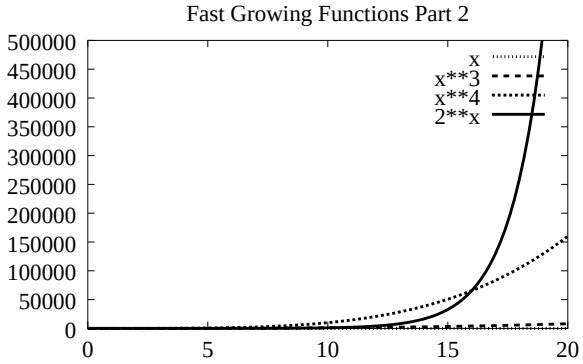


Figure 5.7: Polynomials and an exponential with larger n. Clearly 2^n grows faster than n^4.

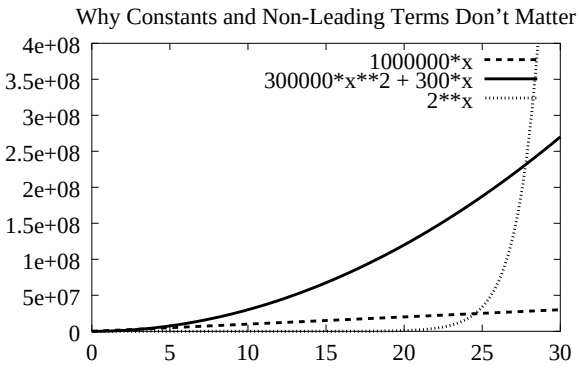


Figure 5.8: Notice that as n gets larger, the constants eventually matter less.

you an accurate picture of the relative growth rates of the functions, they might just as well present a distorted view of the data depending on the values that are used on the axes. Instead, you should use the techniques we develop in this section.

Next we present some of the most important results about the relative growth rate of some common functions. We will ask you to prove each of them. Theorems 5.50 and 5.65 will help you

do so (You may skip those proofs if you did not cover Section 5.1.4). You will notice that most of the theorems are using little-o, not Big-O. Hopefully you understand the difference. If not, review those definitions before continuing.

We begin with something that is pretty intuitive: higher powers grow faster than lower powers.

Theorem 5.76. *Let $a < b$ be real numbers. Then $n^a = o(n^b)$.*

Example 5.77. According to Theorem 5.76, $n^2 = o(n^3)$ and $n^5 = o(n^{5.1})$.

★**Exercise 5.78.** Prove Theorem 5.76. (Hint: Use Theorem 5.50 and do a little algebra before you try to compute the limit. You may skip this Exercise if you did not cover Section 5.1.4.)

The next theorem tells us that exponentials with different bases do not grow at the same rate. More specifically, the higher the base, the faster the growth rate.

Theorem 5.79. *Let $0 < a < b$ be real numbers. Then $a^n = o(b^n)$.*

Example 5.80. According to Theorem 5.79, $2^n = o(5^n)$ and $4^n = o(4.5^n)$.

★**Exercise 5.81.** Prove Theorem 5.79. (See the hint for Exercise 5.78. You may skip this Exercise if you did not cover Section 5.1.4.)

Recall that a logarithmic function is the inverse of an exponential function. That is, $b^x = n$ is equivalent to $x = \log_b n$. The following identity is very useful.

Theorem 5.82. *Let a, b, and x be positive real numbers with $a \neq 1$ and $b \neq 1$. Then*

$$\log_a x = \frac{\log_b x}{\log_b a}.$$

Example 5.83. Most calculators can compute $\ln n$ or $\log_{10} n$, but are unable to compute logarithms with any given base. But Theorem 5.82 allows you to do so. For instance, you can compute $\log_2 39$ as $\log_{10} 39 / \log_{10} 2$.

Notice that the formula in Theorem 5.82 can be rearranged as $(\log_b a)(\log_a x) = \log_b x$. This form should make it evident that changing the base of a logarithm just changes the value by a constant amount. This leads to the following result.

Corollary 5.84. *Let a and b be positive real numbers with $a \neq 1$ and $b \neq 1$.*
Then $\log_a n = \Theta(\log_b n)$.

Proof: *Follows from the definition of Θ and Theorem 5.82.* □

Example 5.85. According to Corollary 5.84, $\log_2 n = \Theta(\log_{10} n)$ and $\ln n = \Theta(\log_2 n)$.

Corollary 5.84 is stating that all logarithms have the same rate of growth regardless of their bases. That is, the base of a logarithm does not matter when it is used in asymptotic notation. Because of this, the base is often omitted in asymptotic notation. In computer science, it is usually safe to assume that the base of logarithms is 2 if it is not specified.

★**Exercise 5.86.** Indicate whether each of the following is *true* (T) or *false* (F).

(a) ___ $2^n = \Theta(3^n)$

(b) ___ $2^n = o(3^n)$

(c) ___ $3^n = O(2^n)$

(d) ___ $\log_3 n = \Theta(\log_2 n)$

(e) ___ $\log_2 n = O(\log_3 n)$

(f) ___ $\log_{10} n = o(\log_3 n)$

Next we see that logarithms grow slower than positive powers of n.

Theorem 5.87. *Let $b > 0$ and $c > 1$ be real numbers. Then $\log_c(n) = o(n^b)$.*

Example 5.88. According to Theorem 5.87, $\log_2 n = o(n^2)$, $\log_{10} n = o(n^{1.01})$, and $\ln n = o(\sqrt{n})$.

★**Exercise 5.89.** Prove Theorem 5.87. (Hint: This is easy if you use Theorems 5.50 and 5.65. You may skip this Exercise if you did not cover Section 5.1.4.)

More generally, the next theorem states that any positive power of a logarithm grows slower than any positive power of n. Since this one is a little tricky, we will provide the proof. In case you have not seen this notation before, you should know that $\log^a n$ means $(\log n)^a$, which is *not* the same thing as $\log(n^a)$.

Theorem 5.90. *Let $a > 0$, $b > 0$, and $c > 0$ be real numbers. Then $\log_c^a(n) = o(n^b)$. In other words, any power of a log grows slower than any polynomial.*

Proof: *First, we need to know that if $a > 0$ is a constant, and $\lim_{n\to\infty} f(n) = C$, then*

$$\lim_{n\to\infty} (f(n))^a = \left(\lim_{n\to\infty} f(n)\right)^a = C^a.$$

Using this and the limit computed in the proof of Theorem 5.87, we have that

$$\lim_{n\to\infty} \frac{\log_c^a(n)}{n^b} = \lim_{n\to\infty} \left(\frac{\log_c(n)}{n^{b/a}}\right)^a = \left(\lim_{n\to\infty} \frac{\log_c(n)}{n^{b/a}}\right)^a = 0^a = 0.$$

Thus, Theorem 5.50 tells us that $\log_c^a(n) = o(n^b)$. □

Example 5.91. According to Theorem 5.90, $\log_2^4 n = o(n^2)$, $\ln^{10} n = o(\sqrt{n})$, and $\log_{10}^{1,000,000} n = o(n^{.00000001})$.

Finally, any exponential function with base larger than 1 grows faster than any polynomial.

Theorem 5.92. *Let $a > 0$ and $b > 1$ be real numbers. Then $n^a = o(b^n)$.*

Example 5.93. According to Theorem 5.92, it is easy to see that $n^2 = o(2^n)$, $n^{15} = o(1.5^n)$, and $n^{1,000,000} = o(1.0000001^n)$.

There are several ways to prove Theorem 5.92, including using repeated applications of l'Hopital's rule, using induction, or doing a little algebraic manipulation and using one of several clever tricks. But the techniques are beyond what we generally need in the course, so we will omit a proof (and, perhaps more importantly, we will not ask you to provide a proof!).

★**Fill in the details 5.94.** Fill in the following blanks with Θ, Ω, O, or o. You should give the most precise answer possible. (e.g. If you put O, but the correct answer is o, your answer is correct but not precise enough.)

(a) $n(n-1) =$ _____$(500n^2)$.

(b) $50n^2 =$ _____$(.001n^4)$.

(c) $\log_2 n =$ _____$(\ln n)$.

(d) $\log_2\left(n^2\right) =$ _____$(\log_2^2(n))$.

(e) $2^{n-1} =$ _____(2^n).

(f) $5^n =$ _____(3^n).

(g) $(n-1)! =$ _____$(n!)$.

(h) $n^3 =$ _____(2^n).

(i) $\log^{100} n =$ _____(1.01^n).

(j) $\log^{100} n =$ _____$(n^{1.01})$.

An alternative notation for little-o is $\ll$. In other words, $f(n) = o(g(n))$ iff $f(n) \ll g(n)$. This notation is useful in certain contexts, including the following comparison of the growth rate of common functions. The previous theorems in this section provide proofs of some of these relationships. The others are given without proof.

Theorem 5.95. *Here are some relationships between the growth rates of common functions:*

$$c \ll \log n \ll log^2 n \ll \sqrt{n} \ll n \ll n \log n \ll n^{1.1} \ll n^2 \ll n^3 \ll n^4 \ll 2^n \ll 3^n \ll n! \ll n^n$$

You should convince yourself that each of the relationships given in the previous theorem is correct. You should also memorize them or (preferably) understand why each one is correct so you can 'recreate' the theorem.

★**Exercise 5.96.** Give a Θ bound for each of the following functions. You do not need to prove them.

(a) $f(n) = n^5 + n^3 + 1900 + n^7 + 21n + n^2$

(b) $f(n) = (n^2 + 23n + 19)(n^2 + 23n + n^3 + 19)n^3$ (Don't make this one harder than it is)

(c) $f(n) = n^2 + 10,000n + 100,000,000,000$

(d) $f(n) = 49 * 2^n + 34 * 3^n$

(e) $f(n) = 2^n + n^5 + n^3$

(f) $f(n) = n \log n + n^2$

(g) $f(n) = \log^{300} n + n^{.000001}$

(h) $f(n) = n! \log n + n^n + 3^n$

★**Exercise 5.97.** Rank the following functions in increasing rate of growth. Clearly indicate if two or more functions have the same growth rate. Assume the logs are base 2.

x, x^2, 2^x, 10000, $\log^{300} x$, x^5, $\log x$, $x^{\log 3}$, $x^{.000001}$, 3^x, $x \log(x)$, $\log(x^{300})$, $\log(2^x)$

5.3 Mathematical Induction

Let's begin our study of mathematical induction (often just called induction) with an example that should look familiar. It is actually Theorem 3.28 that we proved in an earlier chapter. Following that, we will explain how/why induction works and give plenty of other examples.

Example 5.98. Let A be a set with n elements. Prove that $|P(A)| = 2^n$.

> **Proof:** We use induction and the idea from the solution to Exercise 3.24. Clearly if $|A| = 1$, A has $2^1 = 2$ subsets: $\varnothing$ and A itself.
> Assume every set with $n-1$ elements has 2^{n-1} subsets. Let A be a set with n elements. Choose some $x \in A$. Every subset of A either contains x or it doesn't. Those that do not contain x are subsets of $A \setminus \{x\}$. Since $A \setminus \{x\}$ has $n-1$ elements, the induction hypothesis implies that it has 2^{n-1} subsets. Every subset that does contain x corresponds to one of the subsets of $A \setminus \{x\}$ with the element x added. That is, for each subset $S \subseteq A \setminus \{x\}$, $S \cup \{x\}$ is a subset of A containing x. Clearly there are 2^{n-1} such new subsets. Since this accounts for all subsets of A, A has $2^{n-1} + 2^{n-1} = 2^n$ subsets. □

Now we will go into detail about how and why induction works. You should come back and reread Example 5.98 after reading section 5.3.1.

5.3.1 The Basics

The *principle of mathematical induction* (*PMI*, or simply *induction*) is usually used to prove statements of the form

$$\text{for all } n \geq a, P(n) \text{ is true,}$$

where a is an integer, and $P(n)$ is a propositional function with domain $\{a, a+1, a+2, \ldots\}$. Usually a is 0 or 1, so the domain is usually $\mathbb{N}$ (the natural numbers) or $\mathbb{Z}^+$ (the positive integers).

Induction is based on the following fairly intuitive observation (which we will formalize next). Suppose that we are to perform a task that involves a certain number of steps. Suppose that these steps must be followed in strict numerical order. Finally, suppose that we know how to perform the n-th task provided we have accomplished the $(n-1)$-th task. Thus if we are ever able to start the job (that is, if we have a base case), then we should be able to finish it (because starting with the base case we go to the next case, and then to the case following that, etc.).

★**Exercise 5.99.** Based on the description so far, which of the following statements *might* we be able to prove with mathematical induction (indicate with 'Y' or 'N')? Briefly justify.

(a) ___The square of any integer is positive.

(b) ___Every positive integer can be written as the sum of two other positive integers.

(c) ___Every integer greater than 1 can be written as the product of prime numbers.

(d) ___If $n \geq 1$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

(e) ___Every real number is the square of another real number.

The following example illustrates the idea behind induction. It uses *modus ponens*. Recall that modus ponens states that if p is true and $p \to q$ is true, then q is true. In English, "If p is true, and whenever p is true q is true, then q is true."[1]

Example 5.100. Assume that we know that $P(1)$ is true and that whenever $k \geq 1$, $P(k) \to P(k+1)$ is true. What can we conclude?

Solution: Let's start from the ground up. We know that $P(1)$ is true. We also know that $P(k) \to P(k+1)$ is true for any integer $k \geq 1$. For instance, since $4 \geq 1$, we know that $P(4) \to P(5)$ is true. It should be noted that we don't (yet) know anything about the truth values of $P(4)$ and $P(5)$.

- We know $P(1)$ is true and $1 \geq 1$, $P(1) \to P(2)$ is true, therefore $P(2)$ is true.
- Since $P(2)$ is true and $2 \geq 1$, $P(2) \to P(3)$ is true, therefore $P(3)$ is true.
- Since $P(3)$ is true and $3 \geq 1$, $P(3) \to P(4)$ is true, therefore $P(4)$ is true.
- Since $P(4)$ is true and $4 \geq 1$, $P(4) \to P(5)$ is true, therefore $P(5)$ is true.
- Since $P(5)$ is true and $5 \geq 1$, $P(5) \to P(6)$ is true, therefore $P(6)$ is true.

It seems pretty clear that this pattern continues for all values of $k > 6$ as well, so $P(k)$ is true for all $k \geq 1$.

★**Question 5.101.** Example 5.100 had several statements like the following:

"Since $P(4)$ is true and $4 \geq 1$, $P(4) \to P(5)$ is true, therefore $P(5)$ is true."

What is the justification for the conclusion that $P(5)$ is true?

Answer _____

Example 5.100 did not give a formal *proof* of the conclusion. The idea is to get you thinking about how mathematical induction works, not to provide a formal proof that it does (yet). Hopefully this example will help prime your brain for the proof that mathematical induction is a valid proof technique that we will give shortly.

Before moving on, we should make sure you understand what has already been said.

[1] We can also write this as the tautology $[p \wedge (p \to q)] \to q$.

★**Question 5.102.** If you know that $P(5)$ is true, and you also know that $P(k) \to P(k+1)$ whenever $k \geq 1$, what can you conclude?

Answer _____

★**Question 5.103.** If you know that $P(17)$ is true and you also know that $P(k) \to P(k+1)$ whenever $k \geq 1$, what can you conclude about $P(10)$?

Answer _____

Now it is time to get more formal with our discussion. Mathematical induction is based on the fact that if $P(a)$ is true for some $a \geq 0$ (the *base case*), and for any $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true (the *inductive case*), then $P(n)$ is true for all $n \geq a$. In other words, the principle of mathematical induction is based on the fact that

$$[P(a) \wedge \forall k(P(k) \to P(k+1))] \to (\forall n P(n)),$$

where the universe is $\{a, a+1, a+2, \ldots\}$, is true.

★**Exercise 5.104.** Restate $[P(a) \wedge \forall k(P(k) \to P(k+1))] \to (\forall n P(n))$ (where the universe is $\{a, a+1, a+2, \ldots\}$) in English.

Answer _____

_____

_____

The proof that $[P(a) \wedge \forall k(P(k) \to P(k+1))] \to (\forall n P(n))$ is true is based on something called the *well-ordering principle* which states that every nonempty subset of the natural numbers has a least element. Read the following proof very carefully, making sure you understand the justification of every step. If you are not sure about any of the steps, it is important that you get them clarified!

Theorem 5.105. *Assume we are working over the universe* $\{a, a+1, a+2, \ldots\}$. *The statement* $[P(a) \wedge \forall k(P(k) \to P(k+1))] \to (\forall n P(n))$ *is true.*

> **Proof:** *If the statement is false, then it must be that* $P(a) \wedge \forall k(P(k) \to P(k+1))$ *is true but that* $\forall n P(n)$ *is false. Let* $S = \{s \in \{a, a+1, a+2, \ldots\} | \neg P(s)\}$. *That is,* S *is the set of integers for which* $P(n)$ *is false. Since* $\forall n P(n)$ *is false,* S *is nonempty. Clearly* S *is a subset of the natural numbers, so the well-ordering principle applies. Therefore there is some least element* $b \in S$. *Since* $b \in S$, $P(b)$ *is false, and since it is the least such element,* $b - 1 \notin S$, *so* $P(b-1)$ *is true. But we know that* $\forall k(P(k) \to P(k+1))$ *is true, so* $P(b-1) \to P(b)$. *By modus ponens,* $P(b)$ *is true, a contradiction. Therefore the statement is true.* □

It is definitely worth your time to convince yourself that mathematical induction is a valid technique. If you aren't convinced, reread the proof, think about it some more, and/or ask someone to help you understand it.

★**Question 5.106.** Are you convinced that $[P(a) \wedge \forall k(P(k) \to P(k+1))] \to (\forall n P(n))$ is true?

Answer _____

We call $P(a)$ the *base case*. Sometimes we actually need to prove several base cases (we will see why later). For instance, we might need to prove $P(a)$, $P(a+1)$, and $P(a+2)$ are all true.

The *inductive step* involves proving that $\forall k(P(k) \to P(k+1))$ is true. To prove it, we show that if $P(k)$ is true for any k which is *at least as large as the base case(s)*, then $P(k+1)$ is true. The assumption that $P(k)$ is true is called the *inductive hypothesis*.

Based on our discussion so far, here is the procedure for writing induction proofs.

Procedure 5.107. *To use induction to prove that $\forall n P(n)$ is true on domain $\{a, a+1, \ldots\}$:*

1. **Base Case:** *Show that $P(a)$ is true (and possible one or more additional base cases).*
2. *Show that $\forall k(P(k) \to P(k+1))$ is true. To show this:*
   (a) **Inductive Hypothesis:** *Let $k \geq a$ be an integer and assume that $P(k)$ is true.*
   (b) **Inductive Step:** *Prove that $P(k+1)$ is true, typically using the fact that $P(k)$ is true.*

   Assuming we used no special facts about k other than $k \geq a$, this means we have shown that $\forall k(P(k) \to P(k+1))$ (again, where it is understood that the domain is $\{a, a+1, \ldots\}$).
3. **Summary:** *Conclude that $\forall n P(n)$ is true, usually by saying something like "Since $P(a)$ and $P(k) \to P(k+1)$ for all $k \geq a$, $\forall n P(n)$ is true by induction."*

As you will quickly learn, the *base case* is generally pretty easy, as is writing down the *inductive hypothesis*. The *summary* is even easier, since it almost always says the same thing. The *inductive step* is the longest and most complicated step. In fact, in mathematics and theoretical computer science journals, induction proofs often only include the inductive step since anyone reading papers in such journals can generally fill in the details of the other three parts. But keep in mind that you are not (yet) writing papers for such journals, so you *cannot* omit these steps!

Let's see another example.

Example 5.108. Prove that the sum of the first n odd integers is n^2. That is, show that $\sum_{i=1}^{n}(2i-1) = n^2$ for all $n \geq 1$.

Proof: Let $P(n)$ be the statement "$\sum_{i=1}^{n}(2i-1) = n^2$". We need to show that $P(n)$ is true for all $n \geq 1$.

Base Case: Since $\sum_{i=1}^{1}(2i-1) = 2 \cdot 1 - 1 = 1 = 1^2$, $P(1)$ is true.

Inductive Hypothesis: Let $k \geq 1$ and assume that $P(k)$ is true. That is, assume

that $\sum_{i=1}^{k}(2i-1) = k^2$ when $k \geq 1$.

Inductive Step: Then

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \sum_{i=1}^{k}(2i-1) + (2(k+1)-1) \quad \text{(take } k+1 \text{ term from sum)} \\ &= k^2 + (2k+2-1) \quad \text{(by the } \textit{inductive hypothesis}\text{)} \\ &= k^2 + 2k + 1 \\ &= (k+1)^2\end{aligned}$$

Thus $P(k+1)$ is true.

Summary: Since we proved that $P(1)$ is true, and that $P(k) \to P(k+1)$ whenever $k \geq 1$, $P(n)$ is true for all $n \geq 1$ by the principle of mathematical induction. □

The previous proof had the four components we discussed. We proved the *base case*. We then assumed it was true for k. That is, we made the *inductive hypothesis*. Next we proved that it was true for $k+1$ based on the assumption that it is true for k. That is, we did the *inductive step*. Finally, we appealed to the principle of mathematical induction in the *summary*.

Note: *Recall the following statement from Example 5.108:*

Let $P(n)$ be the statement "$\sum_{i=1}^{n}(2i-1) = n^2$".

Did you notice the quotes? It is important that you include these. This is particularly important if you use notation such as $P(n) =$ "$\sum_{i=1}^{n}(2i-1) = n^2$". Without the quotes, this becomes $P(n) = \sum_{i=1}^{n}(2i-1) = n^2$, which is defining $P(n)$ to be $\sum_{i=1}^{n}(2i-1)$ and saying that it is also equal to n^2. These are **not** *saying the same thing. With the quotes, $P(n)$ is a propositional function. Without them, it is a function from $\mathbb{Z}$ to $\mathbb{Z}$.*

In fact, to avoid this confusion, I recommend that you never use the equals sign with propositional functions, especially when writing induction proofs.

Now it's your turn to try to fill in the details of an induction proof.

★**Fill in the details 5.109.** Reprove Theorem 4.50 using induction. That is, prove that for $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof: Let $P(k)$ be the statement "$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$". We need to show that $P(n)$ is true for all $n \geq 1$.

Base Case: When $k = 1$, we have $\sum_{i=1}^{1} i = 1 =$ _____. Therefore,

_____.

Inductive Hypothesis: Let $k \geq 1$, and assume that _____.

That is, assume that _____.

[This is not part of the proof, but it will help us see what's next. Our goal in the next step is to prove that _____ is true. That is, we need to show that _____.]

Inductive Step: Notice that

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \underline{\qquad\qquad} + (k+1) \\
&= \underline{\qquad\qquad} + (k+1) \text{(by the inductive hypothesis)} \\
&= (k+1)\underline{\left(\qquad\qquad\right)} \\
&= \underline{\qquad\qquad}
\end{aligned}$$

Thus, _____.

Summary: We showed that _____ and that whenever _____, $P(k) \to P(k+1)$, therefore $P(n)$ is true for _____ by _____

□

5.3.2 Equalities/Inequalities

The last few example induction proofs have dealt with statements of the form

$$LHS(k) = RHS(k),$$

where LHS stands for *left hand side* and RHS stands for *right hand side*. For instance, in Example 5.108, the statement was

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

so $LHS(k) = \sum_{i=1}^{k}(2i-1)$ and $RHS(k) = k^2$.

★**Question 5.110.** Let $P(n)$ be the statement "$\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$." Determine each of the following:

(a) $P(k)$ is the statement _____.

(b) $P(k+1)$ is the statement _____.

(c) $LHS(k) =$ _____

(d) $RHS(k) =$ _____

(e) $LHS(k+1) =$ _____

(f) $RHS(k+1) =$ _____

For statements of this form, the goal of the inductive step is to show that $LHS(k+1) = RHS(k+1)$ given the fact that $LHS(k)$=$RHS(k)$ (the inductive hypothesis). The way this should generally be done is as follows:

Procedure 5.111. *Given a proposition of the form "$LHS(n) = RHS(n)$," the algebra in the inductive step of an induction proof should be done as follows:*

$LHS(k+1)$	$=$	$LHS(k) + stuff$	*(apply algebra to separate $LHS(k)$ from the rest)*
	$=$	$RHS(k) + stuff$	*(use the inductive hypothesis to replace $LHS(k)$ with $RHS(k)$)*
	$=$	$\cdots$	*(1 or more steps, usually involving algebra, that*
	$=$	$RHS(k+1)$	*result in the goal of getting to $RHS(k+1)$)*

The last few examples followed this procedure, and your proofs should also follow it. Notice that these examples *do not* begin the inductive step by writing out $LHS(k+1) = RHS(k+1)$. One of them wrote it out, but it was *before* the inductive step for the purpose of making the goal in the inductive step clear. The inductive step should always begin by writing just $LHS(k+1)$, and should then use algebra, the inductive hypothesis, etc., until $RHS(k+1)$ is obtained.

This technique also works (with the appropriate slight modifications) with inequalities, e.g.

$$LHS(k) \leq RHS(k) \text{ and}$$

$$LHS(k) \geq RHS(k).$$

For instance, if $P(k)$ is the statement "$k > 2^k$", $LHS(k) = k$, and $RHS(k) = 2^k$. In addition, the '$+stuff$' is not always literally addition. For instance, it might be $LHS(k) \times stuff$.

Here is another example of this type of induction proof–this time using an inequality.

Example 5.112. Prove that $n < 2^n$ for all integers $n \geq 1$.

Proof: Let $P(n)$ be the statement "$n < 2^n$". We want to prove that $P(n)$ is true for all $n \geq 1$.

Base Case: Since $1 < 2^1$, $P(1)$ is clearly true.

Hypothesis: We assume $P(k)$ is true if $k \geq 1$. That is, $k < 2^k$.

Next we need to show that $P(k+1)$ is true. That is, we need to show that $(k+1) < 2^{k+1}$. (Notice that I did not state that this was true, and I do not start with this statement in the next step. I am merely pointing out what I need to prove.*) This paragraph is not really part of the proof–think of it as a side-comment or scratch work.*

Inductive: Given that $k < 2^k$, we can see that

$$\begin{array}{rcll} k+1 & < & 2^k + 1 & (\text{since } k < 2^k) \\ & < & 2^k + 2^k & (\text{since } 1 < 2^k \text{ when } k \geq 1) \\ & = & 2(2^k) & \\ & = & 2^{k+1} & \end{array}$$

Since we have shown that $k+1 < 2^{k+1}$, $P(k+1)$ is true.

Summary: Since we proved that $P(1)$ is true, and that $P(k) \to P(k+1)$, by *PMI*, $P(n)$ is true for all $n \geq 1$. □

In the previous example, $LHS(k) = k$, so $LHS(k+1)$ is already in the form $LHS(k) + stuff$ since $LHS(k+1) = k+1 = LHS(k) + 1$. So the first step of algebra is unnecessary and we were able to apply the inductive hypothesis immediately. Don't let this confuse you. This is essentially the same as the other examples minus the need for algebra in the first step.

Note: *By the time you are done with this section, you will likely be tired of hearing this, but since it is the most common mistake made in induction proofs, it is worth repeating* ad nauseam. **Never begin the inductive step of an induction proof by writing down $\mathbf{P(k+1)}$.** *You do not know it is true yet, so it is not valid to write it down as if it were true so that you can use a technique such as working both sides to verify that it is true (which, as we have also previously stated, is not a valid proof technique).*

You **can** *(and sometimes* **should***) write down $P(k+1)$ on another piece of paper or with a comment such as "We need to prove that" preceding it so that you have a clear direction for the inductive step.*

If you can complete the next exercise without too much difficulty, you are well on your way to understanding how to write induction proofs.

★**Exercise 5.113.** Use induction to prove that for all $n \geq 1$, $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

(Hint: Follow the techniques and format of the previous examples and be smart about your algebra and it will go a lot easier. Also, you will need to factor a polynomial in the inductive step, but if you determine what the goal is ahead of time, it shouldn't be too difficult.)

5.3.3 Variations

In this section we will discuss a few slight variations of the details we have presented so far. First we discuss the fact that we do not need to use a propositional function. Then we will discuss a variation regarding the inductive hypothesis.

It is not always necessary to explicitly define $P(k)$ for use in an induction proof. $P(k)$ is used mostly for convenience and clarity. For instance, in the solution to the previous exercise, it allowed us to just say

$$\text{“}P(k) \text{ is true”}$$

instead of saying

$$\text{“}\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}\text{”} \quad \text{(which is long)}$$

or

$$\text{“the statement is true for } k\text{”} \quad \text{(which is a little vague/awkward).}$$

Here is an example that does not use $P(k)$. It also does not label the four parts of the proof. That is perfectly fine. The main reason we have done so in previous examples is to help you identify them more clearly.

Example 5.114. Let f_n be the n-th Fibonacci number. Prove that for all integers $n \geq 1$,

$$f_{n-1}f_{n+1} = f_n^2 + (-1)^n.$$

Proof: For $k = 1$, we have

$$f_0 f_2 = 0 \cdot 1 = 0 = 1 - 1 = 1^2 + (-1)^1 = f_1^2 + (-1)^1,$$

and so the assertion is true for $k = 1$. Suppose $k \geq 1$, and that the assertion is true for k. That is,

$$f_{k-1}f_{k+1} = f_k^2 + (-1)^k.$$

This can be rewritten as

$$f_k^2 = f_{k-1}f_{k+1} - (-1)^k$$

(a fact that we will find useful below). Then

$$\begin{aligned}
f_k f_{k+2} &= f_k(f_{k+1} + f_k) && \text{(by definition of } f_n \text{ applied to } f_{k+2}) \\
&= f_k f_{k+1} + f_k^2 \\
&= f_k f_{k+1} + f_{k-1}f_{k+1} - (-1)^k && \text{(by rewritten inductive hypothesis)} \\
&= f_{k+1}(f_k + f_{k-1}) + (-1)^{k+1} \\
&= f_{k+1}f_{k+1} + (-1)^{k+1} && \text{(by the definition of } f_k) \\
&= f_{k+1}^2 + (-1)^{k+1},
\end{aligned}$$

and so the assertion is true for $k + 1$. The result follows by induction. □

★**Exercise 5.115.** Use induction to prove that for all $n \geq 1$,

$$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = 2 + (n-1)2^{n+1}$$

or if you prefer,

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

Do so without using a propositional function. You may label the four parts of your proof, but it is not required.

Example 5.116. Prove the generalized form of DeMorgan's law. That is, show that for any $n \geq 2$, if p_1, p_2, ..., p_n are propositions, then

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) = (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n).$$

We provide several appropriate proofs of this one (and one inappropriate one).

Proof 1: (A typical proof)

Let $P(n)$ be the statement "$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) = (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n)$." We want to show that for all $n \geq 2$, $P(n)$ is true. $P(2)$ is DeMorgan's law, so the base case is true. Assume $P(k)$ is true. Then

$$\begin{array}{rcll} \neg(p_1 \vee p_2 \vee \cdots \vee p_{k+1}) & = & \neg((p_1 \vee p_2 \vee \cdots \vee p_k) \vee p_{k+1}) & \text{associative law} \\ & = & \neg(p_1 \vee p_2 \vee \cdots \vee p_k) \wedge \neg p_{k+1} & \text{DeMorgan's law} \\ & = & (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k) \wedge \neg p_{k+1} & \text{hypothesis} \\ & = & (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k \wedge \neg p_{k+1}) & \text{associative law} \end{array}$$

Thus $P(k+1)$ is true. Since we proved that $P(2)$ is true, and that $P(k) \rightarrow P(k+1)$ if $k \geq 2$, by *PMI*, $P(n)$ is true for all $n \geq 2$. □

Proof 2: (Not explicitly defining/using $P(n)$)

We know that $\neg(p_1 \vee p_2) = (\neg p_1 \wedge \neg p_2)$ since this is simply DeMorgan's law. Assume the statement is true for k. That is, $\neg(p_1 \vee p_2 \vee \cdots \vee p_k) = (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k)$. Then we can see that

$$\begin{array}{rcll} \neg(p_1 \vee p_2 \vee \cdots \vee p_{k+1}) & = & \neg((p_1 \vee p_2 \vee \cdots \vee p_k) \vee p_{k+1}) & \text{associative law} \\ & = & \neg(p_1 \vee p_2 \vee \cdots \vee p_k) \wedge \neg p_{k+1} & \text{DeMorgan's law} \\ & = & (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k) \wedge \neg p_{k+1} & \text{hypothesis} \\ & = & (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k \wedge \neg p_{k+1}) & \text{associative law} \end{array}$$

Thus the statement is true for $k+1$. Since we have shown that the statement is true for $n = 2$, and that whenever it is true for k it is true for $k+1$, by *PMI*, the statement is true for all $n \geq 2$. □

Sometimes it is acceptable to omit the justification in the summary. That is, there isn't necessarily a need to restate what you have proven and you can just jump to the conclusion. So the previous proof could end as follows:

> Thus the statement is true for $k+1$. By *PMI*, the statement is true for all $n \geq 2$.

Proof 3: (common in journal articles, unacceptable for this class)

The result follows easily by induction. □

★**Evaluate 5.117.** Prove that for all positive integers n, $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$.

Solution: Base: $n = 1$

$$\begin{aligned} 1 \cdot 1! &= (1+1)! - 1 \\ 1 &= 2! - 1 \\ 1 &= 1 \end{aligned}$$

Assume $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$ for $n \geq 1$.

Induction:

$$\begin{aligned} \sum_{i=1}^{n+1} i \cdot i! &= \sum_{i=1}^{n} i \cdot i! + (n+1)(n+1)! \\ &= (n+1)! - 1 + (n+1)(n+1)! \\ &= (n+1+1)(n+1)! - 1 \\ &= (n+2)(n+1)! - 1 \\ &= (n+2)! - 1 \end{aligned}$$

Therefore it is true for n. Thus by PMI it is true for $n \geq 1$.

Evaluation _____

_____

_____

The second variation we wish to discuss has to do with the inductive hypothesis/step. In the inductive step, we can replace $P(k) \to P(k+1)$ with $P(k-1) \to P(k)$ as long as we prove the statement for all k *larger than any of the base cases*. In general, we can use whatever index we want for the inductive hypothesis as long as we use it to prove that the statement is true for the next index, and as long as we are sure to cover all of the indices down to the base case. For instance, if we prove $P(k+3) \to P(k+4)$, then we need to show it for all $k+3 \geq a$ (that is, all $k \geq a-3$), assuming a is the base case. Put simply, the assumption we make about the value of k must guarantee that the inductive hypothesis includes the base case(s).

★**Question 5.118.** Consider a 'proof' of $\forall n P(n)$ that shows that $P(1)$ is true and that $P(k) \to P(k+1)$ for $k > 1$. What is wrong with such a proof?

Answer _____

_____

Note: *Whether you assume $P(k)$ or $P(k-1)$ is true, you must specify the values of k precisely based on your choice. For instance, if you assume $P(k)$ is true for all $k > a$, you have a problem. Although you known $P(a)$ is true (because it is a base case), when you assume $P(k)$ is true for $k > a$, the smallest k can be is $a+1$. In other words, when you prove $P(k) \to P(k+1)$, you leave out $P(a) \to P(a+1)$. But that means you can't get anywhere from the base case, so the whole proof is invalid.*

If you are wondering why we would use $P(k-1)$ as the inductive hypothesis instead of $P(k)$, it is because sometimes it makes the proof easier–for instance, the algebra steps involved might be simpler.

Example 5.119. Prove that the expression

$$3^{3n+3} - 26n - 27$$

is a multiple of 169 for all natural numbers n.

Proof: Let $P(k)$ be the statement "$3^{3k+3} - 26k - 27 = 169N$ for some $N \in \mathbb{N}$." We will prove that $P(0)$ is true and that $P(k-1) \to P(k)$.

When $k = 0$, $3^{3\cdot 0+3} - 26 \cdot 0 - 27 = 27 - 27 = 0 = 169 \cdot 0$, so $P(0)$ is true.

Let $k > 0$ and assume $P(k-1)$ is true. That is, there is some $N \in \mathbb{N}$ such that $3^{3(k-1)+3} - 26(k-1) - 27 = 169N$. After a little algebra, this is the same as $3^{3k} - 26k - 1 = 169N$. Then

$$\begin{aligned} 3^{3k+3} - 26k - 27 &= 27 \cdot 3^{3k} - 26k - 27 \\ &= 27 \cdot 3^{3k} + (26-27)26k - 27 \\ &= 27 \cdot 3^{3k} - 27 \cdot 26k - 27 + 26 \cdot 26k \\ &= 27(3^{3k} - 26k - 1) + 676k \\ &= 27 \cdot 169N + 169 \cdot 4k \text{ (By the inductive hypothesis)} \\ &= 169(27 \cdot N + \cdot 4k) \end{aligned}$$

which is divisible by 169. The assertion is thus established by induction. □

★**Question 5.120.** Did you notice that in the previous example we assumed $k > 0$ instead of $k \geq 0$? Why did we do that?

Answer _____

5.3.4 Strong Induction

The form of induction we have discussed up to this point only assumes the statement is true for one value of k. This is sometimes called *weak induction*. In *strong induction*, we assume that the statement is true for all values up to and including k. In other words, with strong induction, the inductive hypothesis involves proving that

$$[P(a) \wedge P(a+1) \wedge \cdots \wedge P(k)] \to P(k+1) \text{ if } k \geq a.$$

This may look more complicated, but practically speaking, there is really very little difference. Essentially, strong induction just allows us to assume *more* than weak induction. Let's see an example of why we might need strong induction.

Example 5.121. Show that every integer $n \geq 2$ can be written as the product of primes.

Proof: Let $P(n)$ be the statement "n can be written as the product of primes." We need to show that for all $n \geq 2$, $P(n)$ is true.

Since 2 is clearly prime, it can be written as the product of one prime. Thus $P(2)$ is true.

Assume $[P(2) \wedge P(3) \wedge \cdots \wedge P(k-1)]$ is true for $k > 2$. In other words, assume all of the numbers from 2 to $k-1$ can be written as the product of primes.

We need to show that $P(k)$ is true. If k is prime, clearly $P(k)$ is true. If k is not prime, then we can write $k = a \cdot b$, where $2 \leq a \leq b < k$. By hypothesis, $P(a)$ and $P(b)$ are true, so a and b can be written as the product of primes. Therefore, k can be written as the product of primes, namely the primes from the factorizations of a and b. Thus $P(k)$ is true.

Since we proved that $P(2)$ is true, and that $[P(2) \wedge P(3) \wedge \cdots \wedge P(k-1)] \rightarrow P(k)$ if $k > 2$, by the principle of mathematical induction, $P(n)$ is true for all $n \geq 2$. That is, every integers $n \geq 2$ can be written as the product of primes. □

Example 5.122. In the country of SmallPesia coins only come in values of 3 and 5 pesos. Show that any quantity of pesos greater than or equal to 8 can be paid using the available coins.

Proof: **Base Case:** Observe that $8 = 3 + 5$, $9 = 3 + 3 + 3$, and $10 = 5 + 5$, so we can pay 8, 9, or 10 pesos with the available coinage.

Inductive Hypothesis: Assume we can pay any value from 8 to $k-1$ pesos, where $k \geq 11$.

Inductive step: The inductive hypothesis implies that we can pay with $k-3$ pesos. We can add to the coins used for $k-3$ pesos a single coin of value 3 in order to pay for k pesos.

Summary: Since we can pay for 8, 9, and 10 pesos, and whenever we can pay for anything between 8 and $k-1$ pesos we can pay for k pesos, the strong form of induction implies that we can pay for any quantity of pesos $n \geq 8$.

Notice that the reason we needed three base cases for this proof was the fact that we looked back at $k-3$, three value previous to the value of interest. If we had only proven it for 8, we would have needed to prove 9 and (more importantly) 10 in the inductive step. But the inductive step doesn't work for 10 since there is no solution for $10 - 3 = 7$ pesos. □

Notice that there is no way we could have used weak induction in either of the previous examples.

5.3.5 Induction Errors

The following examples should help you appreciate why we need to be very precise/careful when writing induction proofs.

Example 5.123. What is wrong with the following (supposed) proof that $a^n = 1$ for $n \geq 0$:

Proof: *Base case:* Since $a^0 = 1$, the statement is true for $n = 0$.

Inductive step: Let $k > 0$ and assume $a^j = 1$ for $0 \leq j \leq k$. Then

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

Summary: Therefore by PMI, $a^n = 1$ for all $n \geq 0$. □

Solution: The base case is correct, and there is nothing wrong with the summary, assuming the inductive step is correct. $a^k = 1$ and $a^{k-1} = 1$ are correct by the inductive hypothesis since we are assuming $k > 0$. The algebra is also correct. So what is wrong? The problem is that when $k = 0$, a^{-1} would be in the denominator. But we don't know whether or not $a^{-1} = 1$. Thus we needed to assume $k > 0$. As it turns out, that is precisely where the problem lies. We proved that $P(0)$ is true and that $P(k) \to P(k+1)$ is true when $k > 0$. Thus, we know that $P(1) \to P(2)$, and $P(2) \to P(3)$, etc., but we never showed that $P(0) \to P(1)$ because, of course, it isn't true. The induction doesn't work without $P(0) \to P(1)$.

★**Evaluate 5.124.** Prove or disprove that all goats are the same color.

Solution: If there is one goat, it is obviously the same color as itself. Let $n \geq 1$ and assume that any collection of n goats are all the same color. Consider a collection of $n+1$ goats. Number the goats 1 through $n+1$. Then goats 1 through n are the same color (since there are n of them) and goats 2 through $n+1$ are the same color (again, since there are n of them). Since goat 2 is in both collections, the goats in both collections are the same color. Thus, all $n+1$ goats are the same color.

Evaluation _____

_____

_____

The next example deals with *binary palindromes*. Binary palindromes can be defined recursively by $\lambda, 0, 1 \in P$, and whenever $p \in P$, then $1p1 \in P$ and $0p0 \in P$. (Note: λ is the notation sometimes used to denote the *empty string*—that is, the string of length 0. Also, $1p1$ means the binary string obtained by appending 1 to the begin and end of string p. Similarly for $0p0$.) Notice that there is 1 palindrome of length 0 (λ), 2 of length 1 (0, 1), 2 of length 2 (00, 11), 4 of length 3 (000, 010, 101, 111), etc.

★**Evaluate 5.125.** Use induction to prove that the number of binary palindromes of length $2n$ (even length) is 2^n for all $n \geq 0$.

Proof 1: Base case: $k = 1$. The total number of palindromes of length $2 = 2$ is $2^1 = 2$. It is true.

Assume the total number of binary palindromes with length $2k$ is 2^k. To form a binary palindrome with length $2(k+1) = 2k+2$, with every element in the set of binary palindromes with length $2k$ we either put (00) or (11) to the end or beginning of it. Therefore, the number of binary palindromes with length $2(k+1)$ is twice as many as the number of binary palindromes with length $2k$, which is $2 \times 2^k = 2^{k+1}$. Thus it is true for $k+1$. By the principle of mathematical induction, the total number of binary palindromes of length $2n$ for $n \geq 1$ is 2^n.

Evaluation _____

Proof 2: For the base case, notice that there is $1 = 2^0$ palindromes of length 0 (the empty string). Now assume it is true for all n. For each consecutive binary number with n bits, you are adding a bit to either end, which multiplies the total number by 2^2 permutations, but for it to be a palindrome, they both have to be either 0 or 1, so it would just be 2 instead, so for binary numbers of length $2k$, there are 2^k palindromes.

Evaluation _____

Proof 3: The empty string is the only string of length 0, and it is a palindrome. Thus there is $1 = 2^0$ palindromes of length 0. Let $2n$ be the length, assume $2n \to 2^n$ palindromes. Now we look at $n+1$ so we know the length is $2n+2$ and it starts and ends with either 0 or 1 and has $2n$ values in between. Both possibilities imply 2^n palindromes, so $2^n + 2^n = 2^{n+1}$.

Evaluation _____

★**Exercise 5.126.** Based on the feedback from the previous Evaluate exercise, construct a proper proof that the number of binary palindromes of length $2n$ is 2^n for all $n \geq 0$.

5.3.6 Summary/Tips

Induction proofs are both intuitive and non-intuitive. On the one hand, when you talk through the idea, it seems to make sense. On the other hand, it almost seems like you are using *circular reasoning*. It is important to understand that induction proofs do *not* rely on circular reasoning. Circular reasoning is when you assume p in order to prove p. But here we are not doing that. We are assuming $P(k)$ and using that fact to prove $P(k+1)$, a different statement. However, we are *not* assuming that $P(k)$ is true for all $k \geq a$. We are proving that ***if we assume that*** $P(k)$ ***is true***, then $P(k+1)$ is true. The difference between these statements may seem subtle, but it is important.

Let's summarize our approach to writing an induction proof. This is similar to Procedure 5.107 except we include several of the unofficial steps we have been using that often come in handy. You are not required to use this procedure, but if you are having a difficult time with induction proofs, try this out. Here is the brief version. After this we provide some further comments about each step.

Procedure 5.127. *A slightly longer approach to writing an induction proof is as follows:*

1. **Define:** *(optional) Define $P(n)$ based on the statement you need to prove.*
2. **Rephrase:** *(optional) Rephrase the statement you are trying to prove using $P(n)$. This step is mostly to help you be clear on what you need to prove.*
3. **Base Case:** *Prove the base case or cases.*
4. **Inductive Hypothesis:** *Write down the inductive hypothesis. Usually it is as simple as "Assume that $P(k)$ is true".*
5. **Goal:** *(optional) Write out the goal of the* inductive step *(coming next). It is usually "I need to show that $P(k+1)$ is true" It can be helpful to explicitly write out $P(k+1)$, although see important comments about this step below. This is another step that is mostly for your own clarity.*
6. **Inductive:** *Prove the* goal *statement, usually using the* inductive hypothesis.
7. **Summary:** *The typical induction summary.*

Here are some comments about the steps in Procedure 5.127.

1. **Define:** $P(n)$ should be a statement about a single instance, not about a series of instances. For example, it should be statements like "$2n$ is even" or "A set with n elements has 2^n subsets." It should *NOT* be of the form "$2n$ is even if $n > 1$," "$n^2 > 0$ if $n \neq 0$," or "For all $n > 1$, a set with n elements has 2^n subsets."

2. **Rephrase:** In almost all cases, the rephrased statement should be "For all $n \geq a$, $P(n)$ is true," where a is some constant, often 0 or 1. If the statement cannot be phrased in this way, induction may not be appropriate.

3. **Base Case:** For most statements, this means showing that $P(a)$ is true, where a is the value from the rephrased statement. Although usually one base case suffices, sometimes one must prove multiple base cases, usually $P(a)$, $P(a+1)$, $\ldots$, $P(a+i)$ for some $i > 0$. This depends on the details of the inductive step.

4. **Inductive Hypothesis:** This is almost always one of the following:

   - Assume that $P(k)$ is true.
   - Assume that $P(k-1)$ is true.
   - Assume that $[P(a) \wedge P(a+1) \wedge \cdots \wedge P(k)]$ is true (strong induction)

   Sometimes it is helpful to write out the hypothesis explicitly (that is, write down the whole statement with k or $k-1$ plugged in).

5. **Goal:** As previously stated, this is almost always "I need to show that $P(k+1)$ is true" (or "I need to show that $P(k)$ is true"). But it can be very helpful to explicitly write out what $P(k+1)$ is so you have a clear direction for the next step. However, *it is very important that you do not just write out $P(k+1)$ without prefacing it with a statement like "I need to show that..."*. Since you are about to prove that $P(k+1)$ is true, you don't know that it is

true yet, so writing it down as if it is a fact is incorrect and confusing. In fact, it is probably better write the goal separate from the rest if the proof (e.g. on another piece of paper).

The goal does not need to be written down and is not really part of the proof. The only purpose of doing so it to help you see what you need to do in the next step. For instance, knowing the goal often helps you to figure out the required algebra steps to get there.

6. **Inductive:** This is the longest, and most varied, part of the proof. Once you get the hang of induction, you will typically only think about two parts of the proof—the base case and this step. The rest will become second nature.

   The inductive step should *not* start with writing down $P(k+1)$. Some students want to write out $P(k+1)$ and work both sides until they get them to be the same. As we have emphasized on several occasions, this is *not* a proper proof technique. You cannot start with something you do not know and then work it until you get to something you do know and then declare it is true.

7. **Summary:** This is easy. It is almost always either:

   > "Since we proved that $P(a)$ is true, and that $P(k) \to P(k+1)$, for $k \geq a$, then we know that $P(n)$ is true for all $n \geq a$ by *PMI*, " or
   >
   > "Since we proved that $P(a)$ is true, and that $[P(a) \wedge P(a+1) \wedge \cdots \wedge P(k)] \to P(k+1)$, for $k \geq a$, $P(n)$ is true for all $n \geq a$ by *PMI*."

   The details change a bit depending on what your inductive hypothesis was (e.g. if it was $P(k-1)$ instead of $P(k)$). Technically speaking, you can just summarize your proof by saying

   > "Thus, $P(n)$ is true for all $n \geq a$ by *PMI*."

   As long as someone can look back and see that you included the two necessary parts of the proof, you do not necessarily need to point them out again.

5.4 Solving Recurrence Relations

Recall that a *recurrence relation* is simply a sequence that is recursively defined. More formally, a recurrence relation is a formula that defines a_n in terms of a_i, for one or more values of $i < n$.[2]

Example 5.128. We previously saw that we can define $n!$ by $0! = 1$, and if $n > 0$, $n! = n \cdot (n-1)!$. This is a recurrence relation for the sequence $n!$.

Similarly, we have seen the Fibonacci sequence several times. Recall that n-th Fibonacci number is given by $f_0 = f_1 = 1$ and for $n > 1$, $f_n = f_{n-1} + f_{n-2}$. This is recurrence relation for the sequence of Fibonacci numbers.

Example 5.129. Each of the following are recurrence relations.

$$\begin{aligned} t_n &= n \cdot t_{n-1} + 4 \cdot t_{n-3} \\ r_n &= r_{n/2} + 1 \\ a_n &= a_{n-1} + 2 \cdot a_{n-2} + 3 \cdot a_{n-3} + 4 \cdot a_{n-4} \\ p_n &= p_{n-1} \cdot p_{n-2} \\ s_n &= s_{n-3} + n^2 - 4n + 32 \end{aligned}$$

We have not given any initial conditions for these recurrence relations. Without initial conditions, we cannot compute particular values. We also cannot solve the recurrence relation uniquely.

Recurrence relations have 2 types of terms: *recursive* term(s) and the *non-recursive* terms. In the previous example, the recursive term of s_n is s_{n-3} and the non-recursive term is $n^2 - 4n + 32$.

★**Question 5.130.** Consider the recurrence relations r_n and a_n from Example 5.129.

(a) What are the *recursive* terms of r_n?

Answer _____

(b) What are the *non-recursive* terms of r_n?

Answer _____

(c) What are the *recursive* terms of a_n?

Answer _____

(d) What are the *non-recursive* terms of a_n?

Answer _____

[2] You might also see recurrence relations written using function notation, like $a(n)$. Although there are technical differences between these notations, you can think of them as being essentially equivalent in this context.

One place recurrence relations are useful is to analyze the running time of recursive algorithms. We won't get too technical yet, but let's see a simple example.

Example 5.131. How many multiplications are required to compute $n!$ using the `factorial` algorithm given below (which is simply based on the definition of $n!$)?

```
int factorial(int n) {
    if(n<=0) {
        return 1;
    } else {
        return n*factorial(n-1);
    }
}
```

Solution: Let M_n be the number of multiplications needed to compute $n!$ using the `factorial` algorithm from above. From the code, it is obvious that $M_0 = 0$. If $n > 0$, the algorithm uses one multiplication and then makes a recursive call to `factorial(n-1)`. By the way we defined M_n, `factorial(n-1)` does M_{n-1} multiplications. Therefore, $M_n = M_{n-1} + 1$.

So the recurrence relation for the number of multiplications is

$$M_n = \begin{cases} 0 & \text{if } n{=}0 \\ M_{n-1} + 1 & \text{if } n > 0. \end{cases}$$

Given a recurrence relation for a_n, you can't just plug in n and get an answer. For instance, if $a_n = n \cdot a_{n-1}$, and $a_1 = 1$, what is a_{100}? The only obvious way to compute it is to compute $a_2, a_3, \ldots, a_{99}$, and then finally a_{100}. That is the reason why *solving* recurrence relations is so important. As mentioned previously, solving a recurrence relation simply means finding a *closed form expression* for it.

Example 5.132. It is not too difficult to see that the recurrence from Example 5.131 has the solution $M_n = n$. To prove it, notice that with this assumption, $M_{n-1} + 1 = (n-1) + 1 = n = M_n$, so the solution is consistent with the recurrence relation.

We can also prove it with induction: We know that $M_0 = 0$, so the base case of $k = 0$ is true. Assume $M_k = k$ for $k \geq 0$. Then we have

$$M_{k+1} = M_k + 1 = k + 1,$$

so the formula is correct for $k + 1$. Thus, by PMI, the formula is correct for all $k \geq 0$.

The last example demonstrates an important fact about recurrence relations used to analyze algorithms. The recursive terms come from when a recursive function calls itself. The non-recursive terms come from the other work that is done by the function, including any splitting or combining of data that must be done.

Example 5.133. Consider the recursive *binary search* algorithm that searches for a value in a sorted list. It saves time by discarding large portions of the list at a time. The idea is simple: Look at the middle value of the list. If it is the value you are looking for, you are done. If it is larger than the value you are looking for, then the value must be in the left half of the list. Otherwise it must be in the right half. In either case, you can discard half of the list, and

continue searching in the other half. More formally, it works as follows:

```
binarySearch(list A, value)
    if (A is empty) {
        return false;     // value not found
    }
    if(middle value of A == value)
       return true;      // value found
    else if(middle value of A < value)    // Search left half
        return binarySearch(left half of A, value)
    else    // Search right half
        return binarySearch(right half of A, value)
```

We want to find a recurrence relation for the worst-case complexity of `binarySearch`.

Solution: Let T_n be the complexity of `binarySearch` for an array of size n. Notice that the only things done in the algorithm are to find the middle element, make a few comparisons, perhaps make a recursive call, and return a value. Aside from the recursive call, the amount of work done is constant, which we will just call 1 operation. Notice that at most one recursive call is made, and that the array passed in is half the size. Therefore $T_n = T_{n/2} + 1$.[a] If we want a base case (which we usually do!), we can use $T_1 = 1$ since the algorithm will simply compare the only element in the array to value and return true or false, and that clearly takes constant time. We'll see how to solve this recurrence shortly.

[a] Technically, the recurrence relation is $T_n = T_{\lfloor n/2 \rfloor} + 1$ since $n/2$ might not be an integer. It turns out that most of the time we can ignore the floors/ceilings and still obtain the correct answer.

It turns out that there is no single general method to solve all recurrences. There are many strategies, however. In the next few sections we will discuss four common techniques: the *substitution method*, the *iteration method*, the *Master Theorem* (or *Master Method*), and the *characteristic equation method* for linear recurrences.

★**Question 5.134.** Let's see if you have been paying attention. What does it mean to solve a recurrence relation?

Answer _____

_____

As we continue our discussion of recurrence relations, you will notice that we will begin to sometimes use the function notation (e.g. $T(n)$ instead of T_n). Both notations are commonly used, with the function notation being more common in computer science, for instance.

5.4.1 Substitution Method

The *substitution method* might be better called the *guess and prove it by induction method*. Why? Because to use it, you first have to figure out what you think the solution is, and then you need to actually prove it. Because of the close tie between recurrence relations and induction, it is the most natural technique to use. Let's see an example.

Example 5.135. Consider the recurrence

$$S(n) = \begin{cases} 1 & \text{when } n = 1 \\ S(n-1) + n & \text{otherwise} \end{cases}$$

Prove that the solution is $S(n) = \dfrac{n(n+1)}{2}$.

Proof: When $n = 1$, $S(1) = 1 = \frac{1(1+1)}{2}$. Assume that $S(k-1) = \frac{(k-1)k}{2}$. Then

$$\begin{aligned} S(k) &= S(k-1) + k \text{ (Definition of } S(k)) \\ &= \frac{(k-1)(k)}{2} + k \text{ (Inductive hypothesis)} \\ &= \frac{k^2 - k}{2} + k \text{ (The rest is just algebra)} \\ &= \frac{k^2 - k + 2k}{2} \\ &= \frac{k^2 + k}{2} \\ &= \frac{k(k+1)}{2}. \end{aligned}$$

By PMI, $S(n) = \frac{n(n+1)}{2}$ for all $n \geq 1$. □

★**Exercise 5.136.** Recall that in Example 5.133, we developed the recurrence relation $T(n) = T(n/2) + 1, T(1) = 1$ for the complexity of `binarySearch`. Use substitution to prove that $T(n) = \log_2 n + 1$ is a solution to this recurrence relation.

Example 5.137. Solve the recurrence

$$H_n = \begin{cases} 1 & \text{when } n = 1 \\ 2H_{n-1} + 1 & \text{otherwise} \end{cases}$$

Proof: Notice that $H_1 = 1$, $H_2 = 2 \cdot 1 + 1 = 3$, $H_3 = 2 \cdot 3 + 1 = 7$, and $H_4 = 2 \cdot 7 + 1 = 15$. It sure looks like $H_n = 2^n - 1$, but now we need to prove it. Since $H_1 = 1 = 2^1 - 1$, we have our base case of $n = 1$. Assume $H_n = 2^n - 1$. Then

$$\begin{aligned} H_{n+1} &= 2H_n + 1 \\ &= 2(2^n - 1) + 1 \\ &= 2^{n+1} - 1, \end{aligned}$$

and the result follows by induction. □

★**Exercise 5.138.** Solve the following recurrence relation and use induction to prove your solution is correct: $A(n) = A(n-1) + 2$, $A(1) = 2$.

5.4.2 Iteration Method

With the iteration method (sometimes called *backward substitution*, we expand the recurrence and express it as a summation dependent only on n and initial conditions. Then we evaluate the summation. Sometimes the closed form of the sum is obvious as we are iterating (so no actual summation appears in our work), while at other times it is not (in which case we *do* end up with an actual summation).

Our first example perhaps has too many steps of algebra, but it never hurts to be extra careful when doing so much algebra. We also don't provide a whole lot of justification or explanation for the steps. We will do that in the next example. It is easier to see the overall idea of the iteration

method if we don't interrupt it with comments. If this example does not make sense, come back to it after reading the next example.

Example 5.139. Solve the recurrence

$$R(n) = \begin{cases} 1 & \text{when } n = 1 \\ 2R(n/2) + n/2 & \text{otherwise} \end{cases}$$

Proof: We have

$$\begin{aligned}
R(n) &= 2R(n/2) + n/2 \\
&= 2(2R(n/4) + n/4) + n/2 \\
&= 2^2R(n/4) + n/2 + n/2 \\
&= 2^2R(n/4) + n \\
&= 2^2(2R(n/8) + n/8) + n \\
&= 2^3R(n/8) + n/2 + n \\
&= 2^3R(n/8) + 3n/2 \\
&= 2^3(2R(n/16) + n/16) + 3n/2 \\
&= 2^4R(n/16) + n/2 + 3n/2 \\
&= 2^4R(n/16) + 2n \\
&\vdots \\
&= 2^kR(n/(2^k)) + kn/2 \\
&= 2^{\log_2 n}R(n/(2^{\log_2 n})) + (\log_2 n)n/2 \\
&= nR(n/n) + (\log_2 n)n/2 \\
&= nR(1) + (\log_2 n)n/2 \\
&= n + (\log_2 n)n/2
\end{aligned}$$

□

Using this method requires a little abstract thinking and pattern recognition. It also requires good algebra skills. Care must be taken when doing algebra, especially with the non-recursive terms. Sometimes you should add/multiply (depending on context) them all together, and other times you should leave them as is. The problem is that it takes experience (i.e. practice) to determine which one is better in a given situation. The key is flexibility. If you try doing it one way and don't see a pattern, try another way.

Here is my suggestion for using this method

1. Iterate enough times so you are certain of what the pattern is. Typically this means at least 3 or 4 iterations.
2. As you iterate, make adjustments to your algebra as necessary so you can see the pattern. For instance, whether you write 2^3 or 8 can make a difference in seeing the pattern.
3. Once you see the pattern, generalize it, writing what it should look like after k iterations.
4. Determine the value of k that will get you to the base case, and then plug it in.
5. Simplify.

★**Question 5.140.** The *iteration method* is probably not a good choice to solve the following recurrence relation. Explain why.

$$T(n) = T(n-1) + 3T(n-2) + n * T(n/3) + n^2, \;\; T(1) = 17$$

Answer _____

_____

_____

Here is an example that contains more of an explanation of the technique.

Example 5.141. Solve the recurrence relation $T(n) = 2T(n/2) + n^3$, $T(1) = 1$.

Solution: We start by backward substitution:

$$\begin{aligned} T(n) &= 2T(n/2) + n^3 \\ &= 2[2T(n/4) + (n/2)^3] + n^3 \\ &= 2[2T(n/4) + n^3/8)] + n^3 \\ &= 2^2T(n/4) + n^3/4 + n^3 \end{aligned}$$

Notice that in the second line we have $(n/2)^3$ and not n^3. This may be more clear if rewrite the formula using k: $T(k) = 2T(k/2) + k^3$. When applying the formula to $T(n/2)$, we have $k = n/2$, so we get

$$T(n/2) = 2T((n/2)/2) + (n/2)^3 = 2T(n/4) + n^3/8.$$

Back to the second line, also notice that the 2 is multiplied by both the $2T(n/4)$ and the $(n/2)^3$ terms. A common error is to lose one of the 2s on the $T(n/4)$ term or miss it on the $(n/2)^3$ term when simplifying. Also, $(n/2)^3 = n^3/8$, not $n^3/2$. This is another common mistake. Continuing,

$$\begin{aligned} T(n) &= \ldots \\ &= 2^2T(n/4) + n^3/4 + n^3 \\ &= 2^2[2T(n/8) + (n/4)^3] + n^3/4 + n^3 \\ &= 2^2[2T(n/8) + n^3/4^3] + n^3/4 + n^3 \\ &= 2^3T(n/8) + n^3/4^2 + n^3/4 + n^3. \end{aligned}$$

By now you should have noticed that I use 2 or more steps for every iteration–I do one substitution and then simplify it before moving on to the next substitution. This helps to ensure I don't make algebra mistakes and that I can write it out in a way that helps me see a pattern.

Next, notice that we can write the last line as

$$2^3T(n/2^3) + n^3/4^2 + n^3/4^1 + n^3/4^0,$$

so it appears that we can generalize this to

$$2^kT(n/2^k) + \sum_{i=0}^{k-1} n^3/4^i.$$

The sum starts at $i = 0$ (not 1) and goes to $k - 1$ (not k). It is easy to get either (or both) of these wrong if you aren't careful. We should be careful to make sure we have seen the correct pattern. Too often I have seen students make a pattern out of 2 iterations. Not only is this not enough iterations to be sure of anything, the pattern they usually come up with only holds for the last iteration they did. The pattern has to match *every* iteration. To be safe, go one more iteration after you identify the pattern to verify that it is correct.

Continuing (with a few more steps shown to make all of the algebra as clear as possible), we get

$$\begin{aligned}
T(n) &= \ldots \\
&= 2^3T(n/2^3) + n^3/4^2 + n^3/4^1 + n^3/4^0 \\
&= 2^3[2T(n/2^4) + (n/2^3)^3] + n^3/4^2 + n^3/4^1 + n^3/4^0 \\
&= 2^3[2T(n/2^4) + n^3/2^9] + n^3/4^2 + n^3/4^1 + n^3/4^0 \\
&= 2^4T(n/2^4) + n^3/2^6 + n^3/4^2 + n^3/4^1 + n^3/4^0 \\
&= 2^4T(n/2^4) + n^3/4^3 + n^3/4^2 + n^3/4^1 + n^3/4^0 \\
&= \ldots \\
&= 2^kT(n/2^k) + \sum_{i=0}^{k-1} n^3/4^i.
\end{aligned}$$

Notice that this *does* seem to match the pattern we saw above. We can evaluate the sum to simplify it a little more:

$$\begin{aligned}
T(n) &= \ldots \\
&= 2^k T(n/2^k) + \sum_{i=0}^{k-1} n^3/4^i \\
&= 2^k T(n/2^k) + n^3 \sum_{i=0}^{k-1} 1/4^i \\
&= 2^k T(n/2^k) + n^3 \sum_{i=0}^{k-1} (1/4)^i \\
&= 2^k T(n/2^k) + n^3 \left(\frac{1-(1/4)^k}{1-1/4} \right) \\
&= 2^k T(n/2^k) + n^3 (4/3)(1-(1/4)^k)
\end{aligned}$$

We are almost done. We just need to find a k that allows us to get rid of the recursion. Thus, we need to determine what value of k makes $T(n/2^k) = T(1) = 1$. In other words, we need k such that

$$n/2^k = 1.$$

This is equivalent to

$$n = 2^k.$$

Taking log (base 2) of both sides, we obtain

$$\log_2 n = \log_2(2^k) = k \log_2 2 = k.$$

So $k = \log_2 n$. We plug in k and use the fact that $2^{\log_2 n} = n$ along with the exponent rules to obtain

$$\begin{aligned}
T(n) &= \ldots \\
&= 2^k T(n/2^k) + n^3 (4/3)(1-(1/4)^k) \\
&= 2^{\log_2 n} T(n/2^{\log_2 n}) + n^3 (4/3)(1-(1/4)^{\log_2 n}) \\
&= nT(1) + n^3 (4/3) \left(1 - \frac{1}{(2^2)^{\log_2 n}} \right) \\
&= n \cdot 1 + n^3 (4/3) \left(1 - \frac{1}{(2^{\log_2 n})^2} \right) \\
&= n + n^3 (4/3) \left(1 - \frac{1}{n^2} \right) \\
&= n + \frac{4}{3} n^3 - \frac{4}{3} n \\
&= \frac{4}{3} n^3 - \frac{1}{3} n.
\end{aligned}$$

So we have that $T(n) = \frac{4}{3} n^3 - \frac{1}{3} n$.

★**Exercise 5.142.** Use iteration to solve the recurrence

$$H(n) = \begin{cases} 1 & \text{when } n = 1 \\ 2H(n-1) + 1 & \text{otherwise} \end{cases}$$

Example 5.143. Give a tight bound for the recurrence $T(n) = T(\sqrt{n}) + 1$, where $T(2) = 1$.

Solution: We can see that

$$\begin{aligned} T(n) &= T(n^{1/2}) + 1 \\ &= T(n^{1/4}) + 1 + 1 \\ &= T(n^{1/8}) + 1 + 1 + 1 \\ &= T(n^{1/2^k}) + k \end{aligned}$$

If we can determine when $n^{1/2^k} = 2$, we can obtain a solution. Taking logs (base 2) on both sides, we get

$$\log_2(n^{1/2^k}) = \log_2 2.$$

We apply the power-inside-a-log rule and the fact that $\log_2 2 = 1$ to get

$$(1/2^k) \log_2 n = 1.$$

Multiplying both sides by 2^k and flipping it around, we get

$$2^k = \log_2 n.$$

Again taking logs, we get

$$k = \log_2 \log_2 n.$$

Therefore,

$$\begin{aligned} T(n) &= T(n^{1/2^{\log_2 \log_2 n}}) + \log_2 \log_2 n \\ &= T(2) + \log_2 \log_2 n \ \text{ (since } n^{1/2^{\log_2 \log_2 n}} = 2 \text{ by the way we chose } k) \\ &= 1 + \log_2 \log_2 n. \end{aligned}$$

Therefore, $T(n) = 1 + \log_2 \log_2 n$.

★**Exercise 5.144.** Use iteration to solve the recurrence relation that we developed in Example 5.133 for the complexity of `binarySearch`:

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

If you can do the following exercise correctly, then you have a firm grasp of the iteration method and your algebra skills are superb. If you have difficulty, keep working at it and/or get some assistance. I strongly recommend that you do your best to solve this one on your own.

★**Exercise 5.145.** Solve the recurrence relation $T(n) = 2T(n-1) + n$, $T(1) = 1$. (Hint: You will need the result from Exercise 5.115.)

5.4.3 Master Theorem

We will omit the proof of the following theorem which is particularly useful for solving recurrence relations that result from the analysis of certain types of recursive algorithms–especially divide-and-conquer algorithms.

Theorem 5.146 (Master Theorem)**.** *Let $T(n)$ be a monotonically increasing function satisfying*

$$\begin{aligned} T(n) &= aT(n/b) + f(n) \\ T(1) &= c \end{aligned}$$

where $a \geq 1$, $b > 1$, and $c > 0$. If $f(n) = \Theta(n^d)$, where $d \geq 0$, then

$$T(n) = \begin{cases} \Theta(n^d) & \text{if } a < b^d \\ \Theta(n^d \log n) & \text{if } a = b^d \\ \Theta(n^{\log_b a}) & \text{if } a > b^d \end{cases}$$

Example 5.147. Use the Master Theorem to solve the recurrence

$$T(n) = 4T(n/2) + n, T(1) = 1.$$

Solution: We have $a = 4, b = 2$, and $d = 1$. Since $4 > 2^1$, $T(n) = \Theta(n^{\log_2 4}) = \Theta(n^2)$ by the third case of the Master Theorem.

Example 5.148. Use the Master Theorem to solve the recurrence

$$T(n) = 4T(n/2) + n^2, T(1) = 1.$$

Solution: We have $a = 4, b = 2$, and $d = 2$. Since $4 = 2^2$, we have $T(n) = \Theta(n^2 \log n)$ by the second case of the Master Theorem.

★**Exercise 5.149.** We saw in Example 5.133 that the complexity of binary search is given by the recurrence relation $T(n) = T(n/2) + 1$, $T(1) = 1$. Use the Master Theorem to solve this recurrence.

Example 5.150. Use the Master Theorem to solve the recurrence

$$T(n) = 4T(n/2) + n^3, T(1) = 1.$$

Solution: Here, $a = 4, b = 2$, and $d = 3$. Since $4 < 2^3$, we have $T(n) = \Theta(n^3)$ by the first case of the Master Theorem.

Wow. That was easy.[3] But the ease of use of the Master Method comes with a cost. Well, two actually. First, notice that we do not get an *exact* solution, but only an *asymptotic bound* on the solution. Depending on the context, this may be good enough. If you need an exact numerical solution, the Master Method will do you no good. In the context of analyzing algorithms, typically we are more interested in the asymptotic behavior, and this technique works great. Second, it only works for recurrences that have the exact form $T(n) = aT(n/b) + f(n)$. It won't even work on similar recurrences, such as $T(n) = T(n/b) + T(n/c) + f(n)$.

★**Exercise 5.151.** Use the Master Theorem to solve the recurrence

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

Example 5.152. Let's redo one from a previous section. Use the Master Theorem to solve the recurrence

$$R(n) = \begin{cases} 1 & \text{when } n = 1 \\ 2R(n/2) + n/2 & \text{otherwise} \end{cases}$$

Solution: Here, we have $a = 2$, $b = 2$, and $d = 1$. Since $2 = 2^1$, $R(n) = \Theta(n^1 \log n) = \Theta(n \log n)$. Recall that in Example 5.139 we showed that $R(n) = n + (\log_2 n)n/2$. Since $n + (\log_2 n)n/2 = \Theta(n \log n)$, our solution is consistent.

★**Exercise 5.153.** Use the Master Theorem to solve the recurrence

$$T(n) = 7T(n/2) + 15n^2/4, T(1) = 1.$$

[3] Almost *too* easy.

★**Question 5.154.** In the solution to the previous exercise, we stated that

'$T(n) = \Theta(n^{\log_2 7})$, which is about $\Theta(n^{2.8})$.'

Why didn't we just say '$T(n) = \Theta(n^{\log_2 7}) = \Theta(n^{2.8})$'?

Answer _____

_____

5.4.4 Linear Recurrence Relations

Definition 5.155. *Let $c_1, c_2, \ldots, c_k$ be real constants and $f : \mathbb{N} \to \mathbb{R}$ a function. A recurrence relation of the form*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n) \tag{5.4}$$

is called a **linear recurrence relation** *(or* **linear difference equation***). If $f(n) = 0$ (that is, there is no non-recursive term), we say that the equation is* **homogeneous***, and otherwise we say the equation is* **nonhomogeneous***.*

The *order* of the recurrence is the difference between the highest and the lowest subscripts.

Example 5.156. $u_n = u_{n-1} + 2$ is of the first order, and $u_n = 9u_{n-4} + n^5$ is of the fourth order.

There is a general technique that can be used to solve linear homogeneous recurrence relations. However, we will restrict our discussion to certain first and second order recurrences.

First Order Recurrences

In this section we will learn a technique to solve some first-order recurrences. We won't go into detail about why the technique works.

Procedure 5.157. *Let $f(n)$ be a polynomial and $a \neq 1$. Then the following technique can be used to solve a first order linear recurrence relations of the form*

$$x_n = ax_{n-1} + f(n).$$

1. *First, ignore $f(n)$. That is, solve the homogeneous recurrence $x_n = ax_{n-1}$. This is done as follows:*
   (a) *'Raise the subscripts', so $x_n = ax_{n-1}$ becomes $x^n = ax^{n-1}$. This is called the* characteristic equation.
   (b) *Canceling this gives $x = a$.*
   (c) *The solution to the homogeneous equation $x_n = ax_{n-1}$ will be of the form $x_n = Aa^n$, where A is a constant to be determined.*
2. *Assume that the solution to the original recurrence relation, $x_n = ax_{n-1} + f(n)$, is of the form $x_n = Aa^n + g(n)$, where g is a polynomial of the same degree as $f(n)$.*

3. Plug in enough values to determine the correct constants for the coefficients of $g(n)$.

This procedure is a bit abstract, so let's just jump into seeing it in action.

Example 5.158. Let $x_0 = 7$ and $x_n = 2x_{n-1}, n \geq 1$. Find a closed form for x_n.

Solution: Raising subscripts we have the characteristic equation $x^n = 2x^{n-1}$. Canceling, $x = 2$. Thus we try a solution of the form $x_n = A2^n$, were A is a constant. But $7 = x_0 = A2^0 = A$ and so $A = 7$. The solution is thus $x_n = 7(2)^n$.

Example 5.159. Let $x_0 = 7$ and $x_n = 2x_{n-1} + 1, n \geq 1$. Find a closed form for x_n.

Solution: By raising the subscripts in the homogeneous equation we obtain $x^n = 2x^{n-1}$ or $x = 2$. A solution to the homogeneous equation will be of the form $x_n = A(2)^n$. Now $f(n) = 1$ is a polynomial of degree 0 (a constant) and so the general solution should have the form $x_n = A2^n + B$. Now, $7 = x_0 = A2^0 + B = A + B$. Also, $x_1 = 2x_0 + 1 = 15$ and so $15 = x_1 = 2A + B$. Solving the simultaneous equations

$$A + B = 7,$$

$$2A + B = 15,$$

Using these equations, we can see that $A = 7 - B$ and $B = 15 - 2A$. Plugging the latter into the former, we have $A = 7 - (15 - 2A) = -8 + 2A$, or $A = 8$. Plugging this back into either equation, we can see that $B = -1$. So the solution is $x_n = 8(2^n) - 1 = 2^{n+3} - 1$.

★**Exercise 5.160.** Let $x_0 = 2, x_n = 9x_{n-1} - 56n + 63$. Find a closed form for this recurrence.

Second Order Recurrences

Let us now briefly examine how to solve some second order recursions.

Procedure 5.161. *Here is how to solve a second-order homogeneous linear recurrence relations of the form*

$$x_n = ax_{n-1} + bx_{n-2}.$$

1. *Find the characteristic equation by "raising the subscripts." We obtain* $x^n = ax^{n-1} + bx^{n-2}$.
2. *Canceling this gives* $x^2 - ax - b = 0$. *This equation has two roots* r_1 *and* r_2.
3. *If the roots are different, the solution will be of the form* $x_n = A(r_1)^n + B(r_2)^n$, *where* A, B *are constants.*
4. *If the roots are identical, the solution will be of the form* $x_n = A(r_1)^n + Bn(r_1)^n$.

Example 5.162. Let $x_0 = 1, x_1 = -1, x_{n+2} + 5x_{n+1} + 6x_n = 0$.

Solution: The characteristic equation is $x^2 + 5x + 6 = (x+3)(x+2) = 0$. Thus we test a solution of the form $x_n = A(-2)^n + B(-3)^n$. Since $1 = x_0 = A + B$, and $-1 = -2A - 3B$, we quickly find $A = 2$, and $B = -1$. Thus the solution is $x_n = 2(-2)^n - (-3)^n$.

Example 5.163. Find a closed form for the Fibonacci recurrence $f_0 = 0, f_1 = 1, f_n = f_{n-1} + f_{n-2}$.

Solution: The characteristic equation is $f^2 - f - 1 = 0$. This has roots $\frac{1 \pm \sqrt{5}}{2}$. Therefore, a solution will have the form

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

The initial conditions give

$$0 = A + B, \text{ and}$$

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

From these two equations, we obtain $A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}$. We thus have

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

★**Exercise 5.164.** Find a closed form for the recurrence $x_0 = 1, x_1 = 4, x_n = 4x_{n-1} - 4x_{n-2}$.

5.5 Reading Comprehension Questions

From Section 5.1

★**Question 5.1.** In words, what does $f(n) = O(g(n))$ mean? What does $f(n) = \Theta(g(n))$ mean?

★**Question 5.2.** Assume $f(n) = O(g(n))$.

(a) Does that mean $f(n) \leq g(n)$ for all values of n? Explain. (Hint: A complete answer should bring up two things.)

(b) Does that mean that $f(n) \leq c\,g(n)$ for some constant c and for all values of n? Explain.

(c) Is it possible that $g(10)$ (for instance) is a lot smaller than $f(10)$? Explain.

★**Question 5.3.** If $f(n) = O(g(n))$, does that imply that $f(n) = \Theta(g(n))$? If so, explain why. If not, give an example of functions f and g such that $f(n) = O(g(n))$ but $f(n) \neq \Theta(g(n))$.

★**Question 5.4.** If $f(n) = \Theta(g(n))$, does that imply that $f(n) = O(g(n))$? If so, explain why. If not, give an example of functions f and g such that $f(n) = \Theta(g(n))$ but $f(n) \neq O(g(n))$.

★**Question 5.5.** Explain the difference between $f(n) = o(g(n))$ and $f(n) = O(g(n))$.

★**Question 5.6.** If you know that $f(n) = \Theta(g(n))$, does that give you more, less, or the same amount of information about the relationship between f and g than if you knew that $f(n) = O(g(n))$? Explain.

★**Question 5.7.** Give two different proofs that $7n^3 + 4n^2 - 8n + 27 = O(n^3)$. (Do not forget to use Theorem 5.18 when necessary.)

★**Question 5.8.** Prove that $3^n = o(3.1^n)$.

From Section 5.2

★**Question 5.9.** Explain why $n \log n$ grows faster than cn for any constant $c > 0$. That is, explain why $cn = o(n \log n)$. Note that I am not asking for a proof of this, but an explanation of why it makes sense.

★**Question 5.10.** We think of $\log n$ as a slow growing function. Does that mean that given another function $f(n)$, $f(n) \log n$ grows slower than $f(n)$? (In general, if we multiply a function by a slow growing function, does it make the function grow slower?) Explain.

★**Question 5.11.** Rank the following functions in *increasing* order of rate of growth. Clearly indicate if two of the functions have the same growth rate:

$$n^n,\ 7\log_{10} n,\ n^2 + n + 1,\ 7^n,\ 3n^2,\ 2^n,\ n!,\ \log_3 n,\ 7n \log_2 n,\ n^3,\ 27n,\ 8675309,\ n^3 + n^2 \log_e n$$

From Section 5.3

★**Question 5.12.** Why is the base case required in an induction proof?

★**Question 5.13.** The inductive step involves proving that if $P(k)$ is true, then $P(k+1)$ is true. So it almost seems like you are using a statement to prove the same statement–in other words, circular reasoning. Explain why it is not circular reasoning.

★**Question 5.14.** Recall that $[P(a) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow (\forall n P(n))$ is a tautology, where the universe is $\{a, a+1, a+2, \ldots\}$.

(a) Explain in English what this tautology is saying.

(b) Use *modus ponens* to explain what this has to do with induction.

★**Question 5.15.** If I show that $P(0)$ is true and that for all $k > 0$, $P(k) \rightarrow P(k+1)$, then can I conclude that $P(k)$ is true for all $k \geq 0$? Explain.

★**Question 5.16.** Use induction to prove that if $k \geq 1$, then the number of binary strings of length k is 2^k.

★**Question 5.17.** Student A proves that $P(n)$ is true for all $n \geq 1$ by proving that $P(1)$ is true and that if $P(k)$ is true, then $P(k+1)$ is true whenever $k \geq 1$. Student B proves it by proving that $P(1)$ is true and that if $k > 1$, $P(k-1) \rightarrow P(k)$ is true. Which one has a correct proof technique?

★**Question 5.18.** What is the difference between weak and strong induction?

★**Question 5.19.** Come up with an analogy that helps to explain why proof by induction makes sense. (A common one uses dominoes.)

From Section 5.4

★**Question 5.20.** In your own words, what is a recurrence relation?

★**Question 5.21.** What does it mean to *solve* a recurrence relation?

★**Question 5.22.** In a sentence or two, describe how each of the following techniques is used to solve a recurrence relation

(a) Substitution method

(b) Iteration method

(c) Master Theorem

★**Question 5.23.** (a) Give one advantage of the substitution and iteration methods over the Master Theorem.

(b) Give one advantage of the Master Theorem over the substitution and iteration methods.

(c) List one or two downsides of the substitution method.

(d) List one or two downsides of the iteration method.

(e) At least two downsides of the Master Method.

(f) Which of these three techniques would you rather use? Why?

★**Question 5.24.** Why is the topic of solving recurrence relations in the same chapter as mathematical induction?

5.6 Problems

Problem 5.1. Prove Theorem 5.18.

Problem 5.2. Θ can be thought of as a relation on the set of positive functions, where $(f, g) \in \Theta$ iff $f(n) = \Theta(g(n))$. Prove that Θ is an equivalence relation.

Problem 5.3. Rank the following functions in increasing rate of growth. Indicate if two or more functions have the same growth rate.

$$x!,\ x^3,\ x^2 \log x,\ x,\ x^{\log_2 3},\ \sqrt{x},\ 3^x,\ x \log x,\ x^2,\ x^x,\ x^{3/2},\ x^{\log_3 7},\ x \log(x^2),\ x \log(\log(x)),\ \left(\frac{3}{2}\right)^x$$

Problem 5.4. Prove that $3n^3 - 4n^2 + 13n = O(n^3)$

(a) Using the definition of O.

(b) Using limits.

Problem 5.5. Prove that $5n^2 - 7n = \Theta(n^2)$

(a) Using the definition of Θ and/or Theorem 5.18.

(b) Using limits.

Problem 5.6. Prove that $n \log n = o(n^2)$.

Problem 5.7. Prove that $\log(x^2 + x) = \Theta(\log x)$.

Problem 5.8. Prove that $\sqrt{5x^2 + 11x} = \Theta(x)$.

Problem 5.9. Prove that $n^2 = o(1.01^n)$.

Problem 5.10. Use induction to prove that $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$ for all $n \geq 1$.

Problem 5.11. Use induction to prove that for all $n \geq 2$,

$$\sum_{k=2}^{n} \frac{1}{(k-1)k} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}.$$

Problem 5.12. Prove that for all positive integers n, $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$, where f_n is the nth Fibonacci number.

Problem 5.13. Prove the following generalized De Morgan's Law for sets (where $n \geq 2$):

$$\overline{(A_1 \cup A_2 \cup \cdots \cup A_n)} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}.$$

(Note: There is a second law just like it that swaps the $\cap$s and $\cup$s.)

Problem 5.14. Prove that if $n \geq 4$, $n! > 2^n$.

Problem 5.15. Prove that the number of binary palindromes of length $2k+1$ (odd length) is 2^{k+1} for all $k \geq 0$.

Problem 5.16. Prove that a set of size $n \geq 1$ has 2^n subsets.

Problem 5.17. In Example 5.163 we gave a solution to the recurrence $f_n = f_{n-1} + f_{n-2}$, $f_0 = 0$, $f_1 = 1$. Use the substitution method to re-prove this. (Hint: Recall that the roots to the polynomial $x^2 - x - 1 = 0$ are $\frac{1 \pm \sqrt{5}}{2}$. This is equivalent to $x^2 = x + 1$. You will find this helpful in the inductive step of the proof.

Problem 5.18. Explain why the following joke never ends: *Pete and Repete got in a boat. Pete fell off. Who's left?.*

Problem 5.19. Find and prove a solution for each of the following recurrence relations using two different techniques (this will not only help you verify that your solutions are correct, but it will also give you more practice using each of the techniques). *At least one of the techniques must yield an exact formula if possible.*

(a) $T(n) = T(n/2) + n^2$, $T(1) = 1$. (You may assume n is a power of 2.)

(b) $T(n) = T(n/2) + n$, $T(1) = 1$. (You may assume n is a power of 2.)

(c) $T(n) = 2T(n/2) + n^2$, $T(1) = 1$. (You may assume n is a power of 2.)

(d) $T(n) = T(n-1) \cdot T(n-2)$, $T(0) = 1$, $T(1) = 2$.

(e) $T(n) = T(n-1) + n^2$, $T(1) = 1$.

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

Problem 5.20. Give an exact solution for each of the following recurrence relations.

(a) $a_n = 3a_{n-1}$, $a_1 = 5$.

(b) $a_n = 3a_{n-1} + 2n$, $a_1 = 5$.

(c) $a_n = a_{n-1} + 2a_{n-2}$, $a_0 = 2$, $a_1 = 5$.

(d) $a_n = 6a_{n-1} + 9a_{n-2}$, $a_0 = 1$, $a_1 = 2$.

(e) $a_n = -a_{n-1} + 6a_{n-2}$, $a_0 = 4$, $a_1 = 5$.

Problem 5.21. Use the Master Theorem to find a tight bound for each of the following recurrence relations.

(a) $T(n) = 8T(n/2) + 7n^3 + 6n^2 + 5n + 4$.

(b) $T(n) = 3T(n/5) + n^2 - 4n + 23$.

(c) $T(n) = 3T(n/2) + 3$.

(d) $T(n) = T(n/3) + n$.

(e) $T(n) = 2T(2n/5) + n$.

(f) $T(n) = 5T(2n/5) + n$.

Problem 5.22. Prove, using mathematical induction, that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Problem 5.23. Let $A = \begin{bmatrix} 0 & 3 \\ 2 & 0 \end{bmatrix}$. Find, with proof, A^{2003}.

Problem 5.24. (Requires some trig identities you may have forgotten!) Let $A = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$. Prove that for $n \in \mathbb{N}, n \geq 1$, $A^n = \begin{bmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{bmatrix}$. (Do I have to give you a hint to use induction?)

Problem 5.25. Let $A, B \in \mathbf{M}_{n\times n}$ and k be a positive integer such that $A^k = \mathbf{0}_n$. Prove that if $AB = B$ then $B = \mathbf{0}_n$. (Hint: Try induction.)

Problem 5.26. Prove, by means of induction, that for the following $n \times n$ matrix we have

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 3 & 6 & \cdots & \frac{n(n+1)}{2} \\ 0 & 1 & 3 & \cdots & \frac{(n-1)n}{2} \\ 0 & 0 & 1 & \cdots & \frac{(n-2)(n-1)}{2} \\ \vdots & \vdots & \cdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Problem 5.27. Let

$$A = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}.$$

Conjecture a formula for A^n and prove it using induction.

Chapter 6: Counting

In this chapter we provide a very brief introduction to a field called *combinatorics*. We are actually only going to scratch the surface of this very broad and deep subfield of mathematics and theoretical computer science. We will focus on a subfield of combinatorics that is sometimes called *enumeration*. That is, we will mostly concern ourselves with how to count things.

It turns out that combinatorial problems are notoriously deceptive. Sometimes they can seem much harder than they are, and at other times they seem easier than they are. In fact, there are many cases in which one combinatorial problem will be relatively easy to solve, but a very closely related problem that seems almost identical will be very difficult to solve.

When solving combinatorial problems, you need to make sure you fully understand what is being asked and make sure you are taking everything into account appropriately. I used to tell students that combinatorics was easy. I don't say that anymore. In some sense it is easy. But it is also easy to make mistakes.

6.1 The Sum and Product Rules

We begin our study of combinatorial methods with the following two fundamental principles. They are both pretty intuitive. The only difficulty is realizing which one applies to a given situation. If you have a good understanding of what you are counting, the choice is generally pretty clear.

Theorem 6.1 (Sum Rule)**.** *Let $E_1, E_2, \ldots, E_k$, be pairwise finite disjoint sets. Then*

$$|E_1 \cup E_2 \cup \cdots \cup E_k| = |E_1| + |E_2| + \cdots + |E_k|.$$

Another way of putting the sum rule is this: If you have to accomplish some task and you can do it in one of n_1 ways, or one of n_2 ways, etc., up to one of n_k ways, and none of the ways of doing the task on any of the list are the same, then there are $n_1 + n_2 + \cdots + n_k$ ways of doing the task.

Example 6.2. I have 5 brown shirts, 4 green shirts, 10 red shirts, and 3 blue shirts. How many choices do I have if I intend to wear one shirt?

Solution: Since each list of shirts is independent of the others, I can use the sum rule. Therefore I can choose any of my $5 + 4 + 10 + 3 = 22$ shirts.

Example 6.3. How many ordered pairs of integers (x, y) are there such that $0 < |xy| \leq 5$?

Solution: Let $E_k = \{(x, y) \in \mathbb{Z}^2 : |xy| = k\}$ for $k = 1, \ldots, 5$. Then the desired number is

$$|E_1| + |E_2| + \cdots + |E_5|.$$

We can compute each of these as follows:

$$\begin{aligned}
E_1 &= \{(-1,-1),(-1,1),(1,-1),(1,1)\}\\
E_2 &= \{(-2,-1),(-2,1),(-1,-2),(-1,2),(1,-2),(1,2),(2,-1),(2,1)\}\\
E_3 &= \{(-3,-1),(-3,1),(-1,-3),(-1,3),(1,-3),(1,3),(3,-1),(3,1)\}\\
E_4 &= \{(-4,-1),(-4,1),(-2,-2),(-2,2),(-1,-4),(-1,4),(1,-4),\\
&\quad (1,4),(2,-2),(2,2),(4,-1),(4,1)\}\\
E_5 &= \{(-5,-1),(-5,1),(-1,-5),(-1,5),(1,-5),(1,5),(5,-1),(5,1)\}
\end{aligned}$$

The desired number is therefore $4+8+8+12+8=40$.

★**Exercise 6.4.** For dessert you can have cake, ice cream or fruit. There are 3 kinds of cake, 8 kinds of ice cream and 5 different of fruits. How many choices do you have for dessert?

Answer _____

Theorem 6.5 (Product Rule)**.** *Let $E_1, E_2, \ldots, E_k$, be finite sets. Then*

$$|E_1 \times E_2 \times \cdots \times E_k| = |E_1| \cdot |E_2| \cdots |E_k|.$$

Another way of putting the product rule is this: If you need to accomplish some task that takes k steps, and there are n_1 ways of accomplishing the first step, n_2 ways of accomplishing the second step, etc., and n_k ways of accomplishing the kth step, then there are $n_1 n_2 \cdots n_k$ ways of accomplishing the task.

Example 6.6. I have 5 pairs of socks, 10 pairs of shorts, and 8 t-shirts. How many choices do I have if I intend to wear one of each?

Solution: I can think of choosing what to wear as a task broken into 3 steps: I have to choose a pair of socks (5 ways), a pair of shorts (10 ways), and finally a t-shirt (8 ways). Thus I have $5 \times 10 \times 8 = 400$ choices.

★**Exercise 6.7.** If license plates are required to have 3 letters followed by 3 digits, how many license plates are possible?

Answer _____

Example 6.8. The positive divisors of 400 are written in increasing order

$$1, 2, 4, 5, 8, \ldots, 200, 400.$$

How many integers are there in this sequence? How many of the divisors of 400 are perfect squares?

Solution: Since $400 = 2^4 \cdot 5^2$, any positive divisor of 400 has the form $2^a 5^b$ where $0 \le a \le 4$ and $0 \le b \le 2$. Thus there are 5 choices for a and 3 choices for b for a

total of $5 \cdot 3 = 15$ positive divisors.

To be a perfect square, a positive divisor of 400 must be of the form $2^\alpha 5^\beta$ with $\alpha \in \{0, 2, 4\}$ and $\beta \in \{0, 2\}$. Thus there are $3 \cdot 2 = 6$ divisors of 400 which are also perfect squares.

It is easy to generalize Example 6.8 to obtain the following theorem.

Theorem 6.9. *Let the positive integer n have the prime factorization*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where the p_i are distinct primes, and the a_i are integers ≥ 1. If $d(n)$ denotes the number of positive divisors of n, then

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1).$$

★**Exercise 6.10.** Prove Theorem 6.9. (Hint: Follow the idea from Example 6.8.)

★**Question 6.11.** Whether or not you realize it, you used the fact that the p_i were distinct primes in your proof of Theorem 6.9 (assuming you did the proof correctly). Explain where that fact was used (perhaps implicitly).

Answer _____

_____

Example 6.12. What is the value of *sum* after each of the following segments of code?

```
int sum=0;
for(int i=0;i<n;i++) {
    for(int i=0;i<m;i++) {
        sum = sum + 1;
    }
}
```

```
int sum=0;
for(int i=0;i<n;i++) {
    sum = sum + 1;
}
for(int i=0;i<m;i++) {
    sum = sum + 1;
}
```

Solution: In the code on the left, the inner loop executes m times, so every time the inner loop executes, *sum* gets m added to it. The outer loop executes n times, each time calling the inner loop. Therefore m is added to *sum* n times, so $sum = n \times m$ at the end.

In the code on the right, The first loop adds n to *sum*, and then the second loop adds m to *sum*. Therefore, $sum = n + m$ at the end.

The following problem can be solved using the product rule–you just need to figure out how.

★**Exercise 6.13.** The number 3 can be expressed as a sum of one or more positive integers in four ways, namely, as 3, $1 + 2$, $2 + 1$, and $1 + 1 + 1$. Show that any positive integer n can be so expressed in 2^{n-1} ways.

Answer _____

_____

_____

Example 6.14. Each day I need to decide between wearing a t-shirt or a polo shirt. I have 50 t-shirts and 5 polo shirts. I also have to decide whether to wear jeans, shorts, or slacks. I have 5 pairs of jeans, 15 pairs of shorts, and 4 pairs of slacks. How many different choices do I have when I am getting dressed?

Solution: I have $50 + 5 = 55$ choices for a shirt and $5 + 15 + 4 = 24$ choices or pants. So the total number of choices if $55 \cdot 24 = 1320$.

★**Exercise 6.15.** If license plates are required to have 5 characters, each of which is either a digits or a letter, how many license plates are possible?

Answer _____

★**Exercise 6.16.** How many bit strings are there of length n?

Answer _____

Example 6.17. The integers from 1 to 1000 are written in succession. Find the sum of all the digits.

Solution: When writing the integers from 000 to 999 (with three digits), $3 \times 1000 = 3000$ digits are used. Each of the 10 digits is used an equal number of times, so each digit is used 300 times. The the sum of the digits in the interval 000 to 999 is thus

$$(0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9) \cdot 300 = 13500.$$

Therefore, the sum of the digits when writing the integers from 1 to 1000 is $13500 + 1 = 13501$.

★**Fill in the details 6.18.** In C++, identifiers (e.g. variable and function names) can contain only letters (upper and/or lower case), digits, and the underscore character. They may not begin with a digit.[a]

(a) There are $26 + 26 + 1 = 53$ possible identifiers that contain a single character.

(b) There are $53 \cdot (26 + 26 + 10 + 1) = 53 \cdot 63 = 3339$ possible identifiers with two characters.

(c) There are _____ possible identifiers that contain three characters.

(d) There are _____ possible identifiers that contain four characters.

(e) There are _____ possible identifiers that contain k characters.

[a] There are 84 reserved keywords that cannot be used, but we will ignore these for this exercise.

6.2 Pigeonhole Principle

The following theorem seems so obvious that it doesn't need to be stated. However, it often comes in handy in unexpected situations.

Theorem 6.19 (The Pigeonhole Principle)**.** *If n is a positive integer and $n+1$ or more objects are placed into n boxes, then one of the boxes contains at least two objects.*

Notice that the pigeonhole principle is saying that this is true *no matter how the objects are places in the boxes*. In other words, don't assume that $n-1$ boxes have one object and 1 box has 2 objects. It is possible that all $n+1$ objects are in the same box. But no matter how the objects are distributed in the boxes, we can be sure that there is some box with at least two objects.

Example 6.20. In any group of 13 people, there are always two who have their birthday on the same month. Similarly, if there are 32 people, at least two people were born on the same day of the month.

★**Exercise 6.21.** What can you say about the digits in a number that is 11 digits long?

Answer _____

The pigeonhole principle can be generalized.

Theorem 6.22 (The Generalized Pigeonhole Principle)**.** *If n objects are placed into k boxes, then there is at least one box that contains at least $\lceil n/k \rceil$ objects.*

> **Proof:** *Assume not. Then each of the k boxes contains no more than $\lceil n/k \rceil - 1$ objects. Notice that $\lceil n/k \rceil < n/k + 1$ (convince yourself that this is always true). Thus, the total number of objects in the k boxes is at most*
>
> $$k\left(\lceil n/k \rceil - 1\right) < k(n/k + 1 - 1) = n,$$
>
> *contradicting the fact that there are n objects in the boxes. Therefore, some box contains at least $\lceil n/k \rceil$ objects.* □

The tricky part about using the pigeonhole principle is identifying the *boxes* and *objects*. Once that is done, applying either form of the pigeonhole principle is straightforward. Actually, often the trickiest thing is identifying that the pigeonhole principle even applies to the problem you are trying to solve.

Example 6.23. A drawer contains an infinite supply of white, black, and blue socks. What is the smallest number of socks you must take from the drawer in order to be guaranteed that you have a matching pair?

> **Solution:** Clearly I could grab one of each color, so three is not enough. But according the the Pigeonhole Principle, if I take 4 socks, then I will get at least $\lceil 4/3 \rceil = 2$ of the same color (the colors correspond to the boxes). So 4 socks will guarantee a matched pair.
>
> Notice that I showed two things in this proof. I showed that 4 socks was enough,

but I also showed that 3 was not enough. This is important. For instance, 5 is enough, but it isn't the smallest number that works.

★**Exercise 6.24.** An urn contains 28 blue marbles, 20 red marbles, 12 white marbles, 10 yellow marbles, and 8 magenta marbles. How many marbles must be drawn from the urn in order to assure that there will be 15 marbles of the same color? Justify your answer.

Answer _____

_____

_____

★**Exercise 6.25.** You are in line to get tickets to a concert. Each person can get at most 4 tickets. There are only 100 tickets available. The girl behind you in line says "I sure hope there are enough tickets for me. You're lucky, though. You will get as many as you want." What does she know, and under what circumstances will she get any tickets?

Answer _____

_____

_____

The pigeonhole principle is useful in *existence* proofs–that is, proofs that show that something exists without actually identifying it concretely.

Example 6.26. Show that amongst any seven distinct positive integers not exceeding 126, one can find two of them, say a and b, which satisfy

$$b < a \leq 2b.$$

Solution: Split the numbers $\{1, 2, 3, \ldots, 126\}$ into the six sets

$$\{1, 2\}, \{3, 4, 5, 6\}, \{7, 8, \ldots, 13, 14\}, \{15, 16, \ldots, 29, 30\},$$

$$\{31, 32, \ldots, 61, 62\} \text{ and } \{63, 64, \ldots, 126\}.$$

By the Pigeonhole Principle, two of the seven numbers must lie in one of the six sets, and obviously, any such two will satisfy the stated inequality.

Example 6.27. Given any 9 integers whose prime factors lie in the set $\{3, 7, 11\}$ prove that there must be two whose product is a square.

Solution: For an integer to be a square, all the exponents of its prime factorisation must be even. Any integer in the given set has a prime factorisation of the form $3^a 7^b 11^c$. Now each triplet (a, b, c) has one of the following 8 parity patterns: (even, even, even), (even, even, odd), (even, odd, even), (even, odd, odd), (odd, even, even), (odd, even, odd), (odd, odd, even), (odd, odd, odd). In a group of 9 such integers, there must be two with the same parity patterns in the exponents. Take these two. Their product is a square, since the sum of each corresponding exponent will be even.

★**Exercise 6.28.** The nine entries of a 3×3 grid are filled with -1, 0, or 1. Prove that among the eight resulting sums (three columns, three rows, or two diagonals) there will always be two that add to the same number.

Answer _____

_____

_____

Example 6.29. Prove that if five points are taken on or inside a unit square, there must always be two whose distance is no more than $\frac{\sqrt{2}}{2}$.

Solution: Split the square into four congruent squares as shown to the right. At least two of the points must fall into one of the smaller squares. The longest distance between two points in one of the smaller squares is, by the Pythagorean Theorem, $\sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} = \frac{\sqrt{2}}{2}$. Thus, the result holds.

Example 6.30. Given any set of ten natural numbers between 1 and 99 inclusive, prove that there are two distinct nonempty subsets of the set with equal sums of their elements. (Hint: How many possible subsets are there, and what are the possible sums of the elements within the subsets?)

Solution: There are $2^{10} - 1 = 1023$ non-empty subsets that one can form with a given 10-element set. To each of these subsets we associate the sum of its elements. The minimum value that the sum can be for any subset is $1 + 2 + \cdots + 10 = 55$, and the maximum value is $90 + 91 + \cdots + 99 = 945$. Since the number of possible sums is no more than $945 - 55 + 1 = 891 < 1023$, there must be at least two different subsets that have the same sum.

★**Exercise 6.31.** An eccentric old man has five cats. These cats have 16 kittens among themselves. What is the largest integer n for which one can say that at least one of the five cats has n kittens?

Answer _____

_____

★**Evaluate 6.32.** Prove that at a party with at least two people, there are two people who have shaken hands with the same number of people.

Proof 1: There are $n-1$ people 1 person can shake hands with—4 others if there are 5 people at the party. At one given time two people cannot shake hands with 0 people and $n-1$ people simultaneously because there are 4 slots to fill and 5 people therefore by the pigeonhole principle at least two people shake hands with the same number of others.

Evaluation _____

_____

Proof 2: Assume that at a gathering of $n \geq 2$ people, there are no two people who have shaken hands with the same number of people. If there are two people at the gathering they must either shake hands with each other or shake hands with nobody. However, this contradicts the assumption that no two people have shaken hands with the same number of people. Therefore, by contradiction, at a gathering of $n \geq 2$ people, there are at least two people who have shaken hands with the same number of people.

Evaluation _____

_____

Proof 3: Assume that at a gathering of $n \geq 2$ people, there are no two people who have shaken hands with the same number of people. Person n shakes hands with $n-1$ people because you can't shake your own hand. Person $n-1$ then shakes hands with $n-2$ people and so on...until you reach the last person. He shakes hands with no one which fulfills the contradiction.

Evaluation _____

_____

★**Exercise 6.33.** Give a correct proof of the problem stated in Evaluate 6.32.

★**Exercise 6.34.** There are seventeen friends from high school that all keep in touch by writing letters to each other.[a] To be clear, each person writes separate letters to each of the others. In their letters only three different topics are discussed. Each pair only corresponds about one of these topics. Prove that there at least three people who all write to each other about the same topic.

[a] You do know what letters are, right? They are like e-mail, only they are written on paper, are sent to just one person, and are delivered to your physical mail box.

6.3 Permutations and Combinations

Most of the counting problems we will be dealing with can be classified into one of four categories. The categories are determined by two factors: whether or not repetition is allowed and whether or not order matters. After presenting a brief example of each of these categories, we will go into more detail about each in the following four subsections.

Example 6.35. Consider the set $\{a, b, c, d\}$. Suppose we "select" two letters from these four. Depending on our interpretation, we may obtain the following answers.

(a) **Permutations with repetitions.** The *order* of listing the letters is important, and *repetition is* allowed. In this case there are $4 \cdot 4 = 16$ possible selections:

aa	ab	ac	ad
ba	bb	bc	bd
ca	cb	cc	cd
da	db	dc	dd

(b) **Permutations without repetitions.** The *order* of listing the letters is important, and *repetition is not* allowed. In this case there are $4 \cdot 3 = 12$ possible selections:

	ab	ac	ad
ba		bc	bd
ca	cb		cd
da	db	dc	

(c) **Combinations with repetitions.** The *order* of listing the letters is **not** important, and *repetition is* allowed. In this case there are $\dfrac{4 \cdot 3}{2} + 4 = 10$ possible selections:

aa	ab	ac	ad
	bb	bc	bd
		cc	cd
			dd

(d) **Combinations without repetitions.** The *order* of listing the letters is **not** important, and *repetition is not* allowed. In this case there are $\dfrac{4 \cdot 3}{2} = 6$ possible selections:

	ab	ac	ad
		bc	bd
			cd

Although most of the simple types of counting problems we want to solve can be reduced to one of these four, care must be taken. The previous example assumed that we had a set of *distinguishable* objects. When objects are not distinguishable, the situation is more complicated.

6.3.1 Permutations without Repetitions

Definition 6.36. *Let $x_1, x_2, \ldots, x_n$ be n distinct objects. A* **permutation** *of these objects is simply a rearrangement of them.*

Example 6.37. There are 24 permutations of the letters in $MATH$, namely

$$\begin{array}{llllll} MATH & MAHT & MTAH & MTHA & MHTA & MHAT \\ AMTH & AMHT & ATMH & ATHM & AHTM & AHMT \\ TAMH & TAHM & TMAH & TMHA & THMA & THAM \\ HATM & HAMT & HTAM & HTMA & HMTA & HMAT \end{array}$$

★**Exercise 6.38.** List all of the permutations of EAT

Answer _____

_____

Theorem 6.39. *Let $x_1, x_2, \ldots, x_n$ be n distinct objects. Then there are $n!$ permutations of them.*

Proof: *The first position can be chosen in n ways, the second object in $n-1$ ways, the third in $n-2$, etc. This gives*

$$n(n-1)(n-2)\cdots 2 \cdot 1 = n!.$$

□

Example 6.40. Previously we saw that there are $24 = 4!$ permutations of the letters in $MATH$ and $6 = 3!$ permutations of the letters in EAT.

★**Exercise 6.41.** How many permutations are there of the letters in UNCOPYRIGHTABLE?

Answer _____

Let's see some slightly more complicated examples.

Example 6.42. A bookshelf contains 5 German books, 7 Spanish books and 8 French books. Each book is different from one another. How many different arrangements can be done of these books if

(a) we put no restrictions on how they can be arranged?

(b) books of each language must be next to each other?

(c) all the French books must be next to each other?

(d) no two French books must be next to each other?

Solution:

(a) We are permuting $5 + 7 + 8 = 20$ objects. Thus the number of arrangements sought is $20! = 2432902008176640000$.

(b) "Glue" the books by language, this will assure that books of the same language are together. We permute the 3 languages in 3! ways. We permute the German books in 5! ways, the Spanish books in 7! ways and the French books in 8! ways. Hence the total number of ways is $3! \cdot 5! \cdot 7! \cdot 8! = 146313216000$.

(c) Align the German books and the Spanish books first. Putting these $5+7 = 12$ books creates $12+1 = 13$ spaces (we count the space before the first book, the spaces between books and the space after the last book). To assure that all the French books are next each other, we "glue" them together and put them in one of these spaces. Now, the French books can be permuted in 8! ways and the non-French books can be permuted in 12! ways. Thus the total number of permutations is

$$13 \cdot 8! \cdot 12! = 251073478656000.$$

(d) As with (c), we align the 12 German and Spanish books first, creating 13 spaces. To assure that no two French books are next to each other, we put them into these spaces. The first French book can be put into any of 13 spaces, the second into any of 12 remaining spaces, etc., and the eighth French book can be put into any 6 remaining spaces. Now, the non-French books can be permuted in 12! ways. Thus the total number of permutations is

$$13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 12! = 24856274386944000.$$

★**Exercise 6.43.** Telephone numbers in *Land of the Flying Camels* have 7 digits, and the only digits available are $\{0, 1, 2, 3, 4, 5, 7, 8\}$. No telephone number may begin in 0, 1 or 5. Find the number of telephone numbers possible that meet the following criteria:

(a) You may not repeat any of the digits.

Answer _____

(b) You may not repeat the digits and the phone numbers must be odd.

Answer _____

The previous example and exercise should demonstrate that counting often requires thinking about things in different ways depending on the exact situation. This can be tricky, and it is very easy to make mistakes that lead to under or over counting possibilities. As you are solving problems, think very carefully about what you are counting so you don't fall into this trap.

6.3.2 Permutations with Repetitions

We now consider permutations with repeated objects.

Example 6.44. In how many ways may the letters of the word $MASSACHUSETTS$ be permuted to form different strings?

Solution: We put subscripts on the repeats forming

$$MA_1S_1S_2A_2CHUS_3ET_1T_2S_4.$$

There are now 13 distinguishable objects, which can be permuted in 13! different ways by Theorem 6.39. But this counts some arrangements multiple times since in reality the duplicated letters are not distinguishable. Consider a single permutation of all of the distinguishable letters. If I permute the letters A_1A_2, I get the same permutation when ignoring the subscripts. The same thing is true of T_1T_2. Similarly, there are 4! permutations of $S_1S_2S_3S_4$, so there are 4! permutations that look the same (without the subscripts). Since I can do all of these independently, there are 2!2!4! permutations that look identical when the subscripts are removed. This is true of every permutation. Therefore, the actual number of permutations is $\frac{13!}{2! \cdot 4! \cdot 2!} = 64864800$.

The following exercises should help the technique used in the previous example to sink in.

★**Exercise 6.45.** Use an argument similar to that in Example 6.44 to determine the number of permutations in the letters in $TALL$.

Answer _____

_____

★**Exercise 6.46.** List all of the permutations of the letters $TALL$.

Answer _____

_____

★**Exercise 6.47.** How many permutations are there in the letters of $AEEEI$?

Answer _____

_____

★**Exercise 6.48.** List all of the permutations of the letters $AEEEI$.

Answer _____

_____

_____

The arguments from the previous examples and exercises can be generalized to prove the following.

Theorem 6.49. *Let there be k types of objects: n_1 of type 1; n_2 of type 2; etc. Then the number of ways in which these $n_1 + n_2 + \cdots + n_k$ objects can be rearranged is*

$$\frac{(n_1 + n_2 + \cdots + n_k)!}{n_1! \cdot n_2! \cdots n_k!}.$$

Example 6.50. How many permutations of the letters from $MASSACHUSETTS$ contain $MASS$?

Solution: We can consider $MASS$ as one block along with the remaining 9 letters A, C, H, U, S, E, T, T, S. Thus, we are permuting 10 'letters'. There are two S's[a] and two T's and so the total number of permutations sought is

$$\frac{10!}{2! \cdot 2!} = 907200.$$

[a] Remember, the other two S's are part of $MASS$, which we are now treating as a single object.

★**Exercise 6.51.** How many permutations of the letters from the word $ALGORITHMS$ contain $SMITH$?

Answer _____

_____

_____

Example 6.52. In how many ways may we write the number 9 as the sum of three positive integer summands? Here order counts, so, for example, $1 + 7 + 1$ is to be regarded different from $7 + 1 + 1$.

Solution: We need to find the values of a, b, and c such that $a + b + c = 9$, where $a, b, c \in \mathbb{Z}^+$. We will consider triples (a, b, c) listed smallest to largest and

determine how many ways each triple can be reordered. The possibilities are:

(a, b, c)	Number of permutations
$(1, 1, 7)$	$3!/2! = 3$
$(1, 2, 6)$	$3! = 6$
$(1, 3, 5)$	$3! = 6$
$(1, 4, 4)$	$3!/2! = 3$
$(2, 2, 5)$	$3!/2! = 3$
$(2, 3, 4)$	$3! = 6$
$(3, 3, 3)$	$3!/3! = 1$

Thus the number desired is $3 + 6 + 6 + 3 + 3 + 6 + 1 = 28$.

Example 6.53. In how many ways can the letters of the word **MURMUR** be arranged without allowing two of the same letters next to each other?

Solution: If we started with, say , **MU** then the **R** could be arranged in one of the following three ways:

M	**U**	**R**		**R**	

M	**U**	**R**			**R**

M	**U**		**R**		**R**

In the first case there are $2! = 2$ ways of putting the remaining **M** and **U**, in the second there are $2! = 2$ ways and in the third there is only $1!$ way. Thus starting the word with **MU** gives $2 + 2 + 1 = 5$ possible arrangements. In the general case, we can choose the first letter of the word in 3 ways, and the second in 2 ways. Thus the number of ways sought is $3 \cdot 2 \cdot 5 = 30$.[a]

[a] It should be noted that this analysis worked because the three letters each occurred twice. If this was not the case we would have had to work harder to solve the problem.

★**Exercise 6.54.** Telephone numbers in *Land of the Flying Camels* have 7 digits, and the only digits available are $\{0, 1, 2, 3, 4, 5, 7, 8\}$. No telephone number may begin with 0, 1 or 5. Find the number of telephone numbers possible that meet the following criteria:

(a) You may repeat all digits.

Answer _____

(b) You may repeat digits, but the last digit must be even.

Answer _____

(c) You may repeat digits, but the last digit must be odd.

Answer _____

Example 6.55. In how many ways can the letters of the word **AFFECTION** be arranged, keeping the vowels in their natural order and not letting the two **F**'s come together?

Solution: There are $\frac{9!}{2!}$ ways of permuting the letters of **AFFECTION**. The 4 vowels can be permuted in 4! ways, and in only one of these will they be in their natural order. Thus there are $\frac{9!}{2! \cdot 4!}$ ways of permuting the letters of **AFFECTION** in which their vowels keep their natural order. If we treat FF as a single letter, there are 8! ways of permuting the letters so that the F's stay together. Hence there are $\frac{8!}{4!}$ permutations of **AFFECTION** where the vowels occur in their natural order and the FF's are together. In conclusion, the number of permutations sought is

$$\frac{9!}{2! \cdot 4!} - \frac{8!}{4!} = \frac{8!}{4!}\left(\frac{9}{2} - 1\right) = 8 \cdot 7 \cdot 6 \cdot 5 \cdot \frac{7}{2} = 5880.$$

6.3.3 Combinations without Repetitions

Let's begin with some important notation.

Definition 6.56. *Let n, k be non-negative integers with $0 \leq k \leq n$. The* **binomial coefficient** $\binom{n}{k}$ *(read "n choose k") is defined by*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

An alternative notation is $C(n,k)$. This notation is particularly useful when you want to express a binomial coefficient in the middle of text since it doesn't take up two lines.

Note: *Observe that in the last fraction, there are k factors in both the numerator and denominator. Also, observe the boundary conditions*

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{1} = \binom{n}{n-1} = n.$$

Example 6.57. We have

$$\begin{aligned}
\binom{6}{3} &= \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} = 20, \\
\binom{11}{2} &= \frac{11 \cdot 10}{1 \cdot 2} = 55, \\
\binom{12}{7} &= \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7} = 792, \\
\binom{110}{0} &= 1.
\end{aligned}$$

★**Exercise 6.58.** Compute each of the following

(a) $\binom{7}{5} =$ _____

(b) $\binom{12}{2} =$ _____

(c) $\binom{10}{5} =$ _____

(d) $\binom{200}{4} =$ _____

(e) $\binom{67}{0} =$ _____

If there are n kittens and you decide to take k of them home, you also decided *not* to take $n-k$ of them home. This idea leads to the following important theorem.

Theorem 6.59. *If $n, k \in \mathbb{Z}$, with $0 \leq k \leq n$, then*

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

Proof: *Since $k = n-(n-k)$, the result is obvious.* □

Example 6.60.

$$\binom{11}{9} = \binom{11}{2} = 55.$$

$$\binom{12}{5} = \binom{12}{7} = 792.$$

$$\binom{110}{109} = \binom{110}{1} = 110$$

★**Exercise 6.61.** Compute each of the following

(a) $\binom{17}{15} =$ _____

(b) $\binom{12}{10} =$ _____

(c) $\binom{200}{196} =$ _____

(d) $\binom{67}{66} =$ _____

Definition 6.62. *Let there be n distinguishable objects. A k-***combination** *is a selection of k, $(0 \leq k \leq n)$ objects from the n made without regards to order.*

Example 6.63. The 2-combinations from the list $\{X, Y, Z, W\}$ are

$$XY, XZ, XW, YZ, YW, WZ.$$

Notice that YX (for instance) is not on the list because XY is already on the list and order does not matter.

Example 6.64. The 3-combinations from the list $\{X, Y, Z, W\}$ are

$$XYZ, XYW, XZW, YWZ.$$

★**Exercise 6.65.** List the 2-combinations from the list $\{1, 2, 3, 4, 5\}$

Answer _____

_____

Theorem 6.66. *Let there be n distinguishable objects, and let k, $0 \leq k \leq n$. Then the numbers of k-combinations of these n objects is* $\binom{n}{k}$.

Proof: *The number of ways of picking k objects if the order matters is $n(n-1)(n-2)\cdots(n-k+1)$ since there are n ways of choosing the first object, $n-1$ ways of choosing the second object, etc.. Since each k-combination can be ordered in $k!$ ways, the number of ordered lists of size k is $k!$ times the number of k-combinations. Put another way, the number of k-combinations is the number above divided by $k!$. That is, the total number of k-combinations is*

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

□

Example 6.67. From a group of 10 people, we may choose a committee of 4 in $\binom{10}{4} = 210$ ways.

★**Evaluate 6.68.** A family has seven women and nine men. They need five of them to get together to plan a party. If at least one of the five must be a woman, how many ways are there to select the five?

Solution 1: Since one has to be a woman, this is equivalent to selecting four people from a pool of 15, so the answer is $\binom{15}{4}$.

Evaluation _____

_____

Solution 2: There are 7 women to choose from to ensure there is one woman, and then 4 more need to be selected from the remaining 15. There are $\binom{15}{4}$ ways of doing that. Therefore the total number of ways is $\binom{15}{4} + 7$.

Evaluation _____

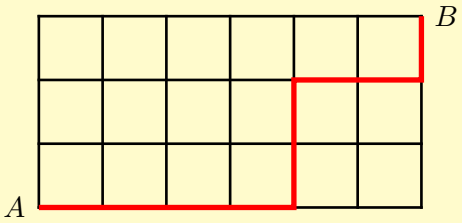
_____

Solution 3: There are $\binom{16}{5}$ possible committees, $\binom{9}{5}$ of which contain only men. Thus, there are $\binom{16}{5} - \binom{9}{5}$ committees that contain at least one woman.

Evaluation _____

_____

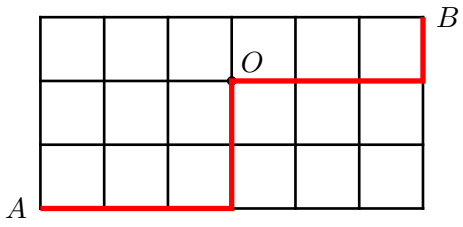
Example 6.69. Consider the following grid:



To count the number of shortest routes from A to B (one of which is given), observe that any shortest path must consist of 6 horizontal moves and 3 vertical ones for a total of $6 + 3 = 9$ moves. Once we choose which 6 of these 9 moves are horizontal the 3 vertical ones are determined. For instance, if I choose to go horizontal on moves 1, 2, 4, 6, 7, and 8, then moves 3, 5 and 9 must be vertical. Since there are 9 moves, I just need to choose which 6 of these are the horizontal moves. Thus there are $\binom{9}{6} = 84$ paths.

Another way to think about it is that we need to compute the number of permutations of $EEEEEENNN$, where E means move east, and N means move north. The number of permutations is $9!/(6! \cdot 3!) = \binom{9}{6}$.

★**Exercise 6.70.** Count the number of shortest routes from A to B that pass through point O in the following grid. (Hint: Break it into two subproblems and combine the solutions.)



★**Evaluate 6.71.** A family has seven women and nine men. How many ways are there to select five of them to plan a party if at least one man and one woman must be selected?

Solution 1: There are 7 choices for the first woman, 9 choices for the first man, and $\binom{14}{3}$ choices for the rest of the committee. Thus, there are $\binom{14}{3} \cdot 7 \cdot 9$ possible committees.

Evaluation _____

_____

Solution 2: Since one has to be a woman and one has to be a man, then they really just need to select 3 more member from the remaining 14 people, so the answer is $\binom{14}{3}$.

Evaluation _____

_____

Now it's your turn to give a correct solution to the previous problem.

★**Exercise 6.72.** A family has seven women and nine men. How many ways are there to select five of them to plan a party if at least one man and one woman must be selected?

★**Question 6.73.** In the answer to the previous problem, we pointed out that two sets of committees did not overlap. Why was that important?

Answer _____

_____

Example 6.74. Three different integers are drawn from the set $\{1, 2, \ldots, 20\}$. In how many ways may they be drawn so that their sum is divisible by 3?

Solution: In $\{1, 2, \ldots, 20\}$ there are

6 numbers leaving remainder 0
7 numbers leaving remainder 1
7 numbers leaving remainder 2

The sum of three numbers will be divisible by 3 when (a) the three numbers are divisible by 3; (b) one of the numbers is divisible by 3, one leaves remainder 1 and the third leaves remainder 2 upon division by 3; (c) all three leave remainder 1 upon division by 3; (d) all three leave remainder 2 upon division by 3. Hence the number of ways is

$$\binom{6}{3} + \binom{6}{1}\binom{7}{1}\binom{7}{1} + \binom{7}{3} + \binom{7}{3} = 384.$$

★**Evaluate 6.75.** The 300-level courses in the CS department are split into three groups: Foundations (361, 385), Applications (321, 342, 392), and Systems (335, 354, 376). In order to get a BS in computer science at Hope you need to take at least one course from each group. If you take four 300-level courses, how many different possibilities do you have that satisfy the requirements?

Solution 1: You have to take one from each group and then you can take any of the remaining 5 courses. So the total is $2 * 3 * 3 * 5 = 90$.

Evaluation _____

_____

Solution 2: $\binom{8}{4} = 70$

Evaluation _____

_____

★**Evaluate 6.76.** Using the same requirements from Evaluate 6.75, how many total ways are there to take 300-level courses that satisfy the requirements?

Solution 1: Take one from each group and then choose between 0 and 5 of the remaining 5. The total is therefore $2 * 3 * 3 * \sum_{k=0}^{5} \binom{5}{k}$.

Evaluation _____

_____

Solution 2: Since you can take anywhere between 3 and 8 courses, the number of possibilities is $\binom{8}{3} + \binom{8}{4} + \binom{8}{5} + \binom{8}{6} + \binom{8}{7} + \binom{8}{8}$.

Evaluation _____

_____

In Problem 6.31 you will have a chance to properly solve the problems from the previous two Evaluate exercises.

6.3.4 Combinations with Repetitions

Example 6.77. How many ways are there to put 10 ping pong balls into 4 buckets?

Solution: We will solve this using a technique sometimes called *bars and stars*. We will represent the drawers with bars and the balls with stars. We will use 10 stars and 3 bars. To see why this is 3 and not 4, let's see how we represent the situation of having 3 balls in the first bucket, 5 in the second, none in the third, and 2 in the fourth:

|**||**

Do you see it? The bars act as separators between the buckets, which is why we have one less bar than the number of buckets.

Given this formulation, aren't we just trying to find all possible orderings of bars and stars? Indeed. To do so, all we need to do is determine where to put the stars, and the bars 'fall into place'. Alternatively, we can determine where to put the bars and let the stars fall into place. There are 13 spots and we need to choose 10 spots for the balls (the 'stars') or 3 spots for the bucket separators (the 'bars'). So the solution is

$$\binom{13}{10} = \binom{13}{3} = 286.$$

Notice that Theorem 6.59 implies that these two methods of solving the problem will always be the same, which is a really good thing.

Example 6.78. How many ways are there to choose 10 pieces of fruit if you can take any number of bananas, oranges, apples, or pears and the order I select them does not matter?

Solution: Again we can use stars and bars so solve this problem. We need 10 stars to represent the chosen fruits and 3 bars to divide the four fruits we can choose from. The stars before the first bar represent bananas, those between the first and second bar are oranges, between the second and third are apples, and after the third are pears. Thus, we need to count the number of ways we can arrange 10 stars and 3 bars. Notice that this is exactly the same thing we did in the previous example, so the answer is

$$\binom{13}{10} = \binom{13}{3} = 286.$$

★**Exercise 6.79.** I want to make a sandwich that has 3 slices of meat. My refrigerator is well stocked because I have 11 different meats to choose from. How many choices do I have for my sandwich if I allow myself to have multiple slices of the same meat and the order the slices appear on the sandwich does not matter?

Answer _____

_____

_____

We can generalize the previous examples as follows.

Theorem 6.80. *There are* $\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$ *ways of placing* k *indistinguishable objects into* n *distinguishable bins.*

This is also the number of ways of selecting k *objects from a collection of* n *objects if repetition is allowed.*

The previous theorem can be applied to various situations. As with the pigeonhole principle, the trickiest part is recognizing when and how to apply it.

6.4 Binomial Theorem

It is well known that

$$(a+b)^2 = a^2 + 2ab + b^2 \tag{6.1}$$

Multiplying this last equality by $a+b$ one obtains

$$(a+b)^3 = (a+b)^2(a+b) = a^3 + 3a^2b + 3ab^2 + b^3$$

Again, multiplying

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \tag{6.2}$$

by $a+b$ one obtains

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

This generalizes, as we see in the next theorem.

Theorem 6.81 (Binomial Theorem)**.** *Let x and y be variables and n be a nonnegative integer. Then*

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

Example 6.82. Expand $(4x+5)^3$, simplifying as much as possible.

Solution:

$$\begin{aligned}(4x+5)^3 &= \binom{3}{0}(4x)^3 5^0 + \binom{3}{1}(4x)^2(5)^1 + \binom{3}{2}(4x)^1(5)^2 + \binom{3}{3}(4x)^0 5^3 \\ &= (4x)^3 + 3(4x)^2(5) + 3(4x)(5)^2 + 5^3 \\ &= 64x^3 + 240x^2 + 300x + 125\end{aligned}$$

Example 6.83. In the following, $i = \sqrt{-1}$, so that $i^2 = -1$.

$$\begin{aligned}(2+i)^5 &= 2^5 + 5(2)^4(i) + 10(2)^3(i)^2 + 10(2)^2(i)^3 + 5(2)(i)^4 + i^5 \\ &= 32 + 80i - 80 - 40i + 10 + i \\ &= -38 + 39i\end{aligned}$$

Notice that we skipped the step of explicitly writing out the binomial coefficient for this example. You can do it either way–just make sure you aren't forgetting anything or making algebra mistakes by taking shortcuts.

★**Exercise 6.84.** Expand $(2x - y^2)^4$, simplifying as much as possible.

The most important things to remember when using the binomial theorem are not to forget the binomial coefficients, and not to forget that the powers (i.e. x^{n-i} and y^i) apply to the whole term, including any coefficients. A specific case that is easy to forget is a negative sign on the coefficient. Did you make any of these mistakes when doing the last exercise? Be sure to identify your errors so you can avoid them in the future.

★**Exercise 6.85.** Expand $(\sqrt{3} + \sqrt{5})^4$, simplifying as much as possible.

Example 6.86. Let $n \geq 1$. Find a closed form for $\displaystyle\sum_{k=0}^{n} \binom{n}{k} (-1)^k$.

Solution: Using a little algebra and the binomial theorem, we can see that

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

★**Exercise 6.87.** Find a closed form for $\displaystyle\sum_{k=1}^{n} \binom{n}{k} 3^k$.

If we ignore the variables in the Binomial Theorem and write down the coefficients for increasing values of n, a pattern, called *Pascal's Triangle*, emerges (see Figure 6.1).

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 \\
 & & & 1 & & 9 & & 36 & & 84 & & 126 & & 126 & & 84 & & 36 & & 9 & & 1 \\
1 & & 10 & & 45 & & 120 & & 210 & & 252 & & 210 & & 120 & & 45 & & 10 & & 1 \\
 & & & & & & \vdots & & & & & & &
\end{array}$$

Figure 6.1: Pascal's Triangle

Notice that each entry (except for the 1s) is the sum of the two neighbors just above it. This observation leads to the Pascal's Identity.

Theorem 6.88 (Pascal's Identity)**.** *Let n and k be positive integers with $k \leq n$. Then*

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

Proof: *See Problem 6.21.* □

6.5 Inclusion-Exclusion

The Sum Rule (Theorem 6.1) gives us the cardinality for unions of finite sets that are mutually disjoint. In this section we will drop the disjointness requirement and obtain a formula for the cardinality of unions of general finite sets.

The Principle of *Inclusion-Exclusion* is attributed to both Sylvester and to Poincaré. We will only consider the cases involving two and three sets, although the principle easily generalizes to k sets.

Theorem 6.89 (Inclusion-Exclusion for Two Sets)**.** *Let A and B be sets. Then*

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

Proof: *Clearly there are $|A \cap B|$ elements that are in both A and B. Therefore, $|A| + |B|$ is the number of element in A and B, where the elements in $|A \cap B|$ are counted twice. From this it is clear that $|A \cup B| = |A| + |B| - |A \cap B|$.* □

Example 6.90. Of 40 people, 28 smoke and 16 chew tobacco. It is also known that 10 both smoke and chew. How many among the 40 neither smoke nor chew?

Solution: Let A denote the set of smokers and B the set of chewers. Then

$$|A \cup B| = |A| + |B| - |A \cap B| = 28 + 16 - 10 = 34,$$

meaning that there are 34 people that either smoke or chew (or possibly both). Therefore the number of people that neither smoke nor chew is $40 - 34 = 6$.

★**Exercise 6.91.** In a group of 100 camels, 46 eat wheat, 57 eat barley, and 10 eat neither. How many camels eat both wheat and barley?

Example 6.92. Consider the set A that are multiples of 2 no greater than 114. That is,

$$A = \{2, 4, 6, \ldots, 114\}.$$

(a) How many elements are there in A?

(b) How many are divisible by 3?

(c) How many are divisible by 5?

(d) How many are divisible by 15?

(e) How many are divisible by either 3, 5 or both?

(f) How many are neither divisible by 3 nor 5?

(g) How many are divisible by exactly one of 3 or 5?

Solution: Let $A_k \subset A$ be the set of those integers divisible by k.

(a) Notice that the elements are $2 = 2(1)$, $4 = 2(2)$, $\ldots$, $114 = 2(57)$. Thus $|A| = 57$.

(b) Notice that

$$A_3 = \{6, 12, 18, \ldots, 114\} = \{1 \cdot 6, 2 \cdot 6, 3 \cdot 6, \ldots, 19 \cdot 6\},$$

so $|A_3| = 19$.

(c) Notice that

$$A_5 = \{10, 20, 30, \ldots, 110\} = \{1 \cdot 10, 2 \cdot 10, 3 \cdot 10, \ldots, 11 \cdot 10\},$$

so $|A_5| = 11$.

(d) Notice that $A_{15} = \{30, 60, 90\}$, so $|A_{15}| = 3$.

(e) First notice that $A_3 \cap A_5 = A_{15}$. Then it is clear that the answer is

$$|A_3 \cup A_5| = |A_3| + |A_5| - |A_{15}| = 19 + 11 - 3 = 27.$$

(f) We want

$$|A \setminus (A_3 \cup A_5)| = |A| - |A_3 \cup A_5| = 57 - 27 = 30.$$

(g) We want

$$\begin{aligned} |(A_3 \cup A_5) \setminus (A_3 \cap A_5)| &= |(A_3 \cup A_5)| - |A_3 \cap A_5| \\ &= 27 - 3 \\ &= 24. \end{aligned}$$

We now derive a three-set version of the Principle of Inclusion-Exclusion.

Theorem 6.93 (Inclusion-Exclusion for Three Sets)**.** *Let A, B, and C be sets. Then*

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad -|A \cap B| - |A \cap C| - |B \cap C| \\ &\quad +|A \cap B \cap C| \end{aligned}$$

Proof: *Using the associativity and distributivity of unions of sets, we see that*

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| \\ &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B \cup C| - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |(A \cap B) \cap (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|) \\ &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|. \ \square \end{aligned}$$

Example 6.94. At *Medieval High* there are forty students. Amongst them, fourteen like Mathematics, sixteen like theology, and eleven like alchemy. It is also known that seven like Mathematics and theology, eight like theology and alchemy and five like Mathematics and alchemy. All three subjects are favored by four students. How many students like neither Mathematics, nor theology, nor alchemy?

Solution: Let A be the set of students liking Mathematics, B the set of students liking theology, and C be the set of students liking alchemy. We are given that

$$|A| = 14, |B| = 16, |C| = 11, |A \cap B| = 7, |B \cap C| = 8, |A \cap C| = 5,$$

and

$$|A \cap B \cap C| = 4.$$

Using Theorem 6.93, along with some set identities, we can see that

$$\begin{aligned} |\overline{A} \cap \overline{B} \cap \overline{C}| &= |\overline{A \cup B \cup C}| \\ &= |U| - |A \cup B \cup C| \\ &= |U| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C| \\ &= 40 - 14 - 16 - 11 + 7 + 5 + 8 - 4 \\ &= 15. \end{aligned}$$

★**Exercise 6.95.** A survey of a group's viewing habits revealed the percentages that watch a given sport. The results are given below. Calculate the percentage of the group that watched none of the three sports.

28% gymnastics	14% gymnastics & baseball	8% all three sports
29% baseball	10% gymnastics & soccer	
19% soccer	12% baseball & soccer	

★**Exercise 6.96.** Would you believe a market investigator that reports that of 1000 people, 816 like candy, 723 like ice cream, 645 like cake, while 562 like both candy and ice cream, 463 like both candy and cake, 470 like both ice cream and cake, while 310 like all three? State your reasons!

Example 6.97. An auto insurance company has 10,000 policyholders. Each policy holder is classified as

- young or old,
- male or female, and
- married or single.

Of these policyholders, 3000 are young, 4600 are male, and 7000 are married. The policyholders can also be classified as 1320 young males, 3010 married males, and 1400 young married persons. Finally, 600 of the policyholders are young married males.

How many of the company's policyholders are young, female, and single?

Solution: Let Y, F, S, M stand for young, female, single, male, respectively, and let Ma stand for married. We have

$$\begin{aligned} |Y \cap F \cap S| &= |Y \cap F| - |Y \cap F \cap Ma| \\ &= |Y| - |Y \cap M| \\ &\qquad -(|Y \cap Ma| - |Y \cap Ma \cap M|) \\ &= 3000 - 1320 - (1400 - 600) \\ &= 880. \end{aligned}$$

The following problem is a little more challenging than the others we have seen, but you have all of the tools you need to tackle it.

★**Exercise 6.98** (Lewis Carroll in *A Tangled Tale.*)**.** In a very hotly fought battle, at least 70% of the combatants lost an eye, at least 75% an ear, at least 80% an arm, and at least 85% a leg. What can be said about the percentage who lost all four members?

6.6 Reading Comprehension Questions

From Section 6.1

★**Question 6.1.** For each of the following, make up an example that requires the given rule to solve. Your example should not just rehash an example from the book. Bonus points if it is computer science related. For each, also give and explain the solution.

(a) The sum rule

(b) The product rule

(c) Both the sum rule and product rule

From Section 6.2

★**Question 6.2.** If there are 12 objects in 10 boxes, does the pigeonhole principle allow you to conclude that one box has at least 3 objects? Or that two boxes have at least two items? Or that every box has at least one item? What is the most precise thing that you can conclude from it?

★**Question 6.3.** Assume 30 balls are placed in 7 bins. Give several different possibilities for how many balls are in each bin, trying to make the examples as different from each other as possible. What is true of all of your examples, as predicted by the generalized pigeonhole principle?

★**Question 6.4.** I have 21 disc golf discs, including putters, approach discs, fairway drivers, and distance drivers. Tell me everything you can say for certain about how many of each type of disc I have.

★**Question 6.5.** Twelve people each pick a number from 1 to 1000. Prove that at least two of them picked numbers that have the same number of 1s in their binary representation or show why it is possible that this is not the case (i.e. give a counterexample).

From Section 6.3

★**Question 6.6.** What is the difference between a permutation and a combination?

★**Question 6.7.** How many are there of each of the following (where *digit* means decimal digit).

(a) Three-digit numbers

(b) Three-digit numbers with no repeated digits

(c) Sets consisting of three digits. (e.g. $\{4, 0, 5\}$)

(d) Lists consisting of three digits. (e.g. $[4, 2, 3]$)

★**Question 6.8.** (a) How many permutations are there of the set $\{8, 6, 7, 5, 3, 0, 9\}$? (b) How many of these permutations begin with 8 and end with 9?

★**Question 6.9.** You know somebody's PIN number uses the digits 3, 3, 6, 6, 8, but you do not know the order. How many possible PIN numbers have these digits?

★**Question 6.10.** You need to choose a team of 45 people out of a possible 50 people. What is probably a much easier way of thinking about this problem?

★**Question 6.11.** Compute $\binom{25}{22}$ by hand. (Hint: Be smart!)

★**Question 6.12.** The board of directors for the Holland Running Club has 11 members. The executive board is a subcommittee of the board of directors consisting of 4 members (from the 11). The executive board consists of the president, vice-president, treasurer, and secretary.

(a) How many different possibilities are there for the executive board if we do not care which office they hold?

(b) If we are given the four members of the executive board, how many ways are there of assigning the offices?

(c) How many different possible executive boards are there (choosing from the whole board) if we *do* care about who is in which office?

★**Question 6.13.** What are two important factors that influence how you go about counting things (i.e. help you determine which technique you will use)?

From Section 6.4

★**Question 6.14.** (a) Simplify $\displaystyle\sum_{k=0}^{n} \binom{n}{k} 10^k$.

(b) Compute the previous sum for $n = 0, 1, 2, 3, 4, 5$. (Hint: Use your solution to part (a)!)

(c) Attempt to make a connection between this question and Pascal's Triangle. It may be a bit subtle, but it is kind of neat if you see it.

★**Question 6.15.** Use the Binomial Theorem to expand $(2x-3y)^5$, simplifying as much as possible.

★**Question 6.16.** Use the Binomial Theorem to prove that $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

From Section 6.5

★**Question 6.17.** A rather large family has 12 children, all who attended college. 6 of them took a math class, 5 took a computer science class, and 4 took neither a math class or a computer science class. How many took both a math and a computer science class?

★**Question 6.18.** In a class of 20 students, 7 show up late and 4 sleep during class. How many students do neither? Give both a minimum and maximum since there is not enough information to know for sure.

★**Question 6.19.** You want to use Inclusion-Exclusion on 3 sets (e.g. your goal is to compute how many things are in the union of 3 sets). You are given 6 pieces of information. Is that enough to solve the problem? Explain.

★**Question 6.20.** Given Inclusion-Exclusion on two and three sets, can you generalize it to four sets? Thus, given sets A, B, C, and D, what is a formula for $|A \cup B \cup C \cup D|$?

6.7 Problems

Problem 6.1. How many license plates can be made using either three letters followed by three digits or four letters followed by two digits?

Problem 6.2. How many license plates can be made using 4 letters and 3 numbers if the letters cannot be repeated and the letters and numbers may appear in any order?

Problem 6.3. How many bit strings of length 8 either begin with three 1s or end with four 0s?

Problem 6.4. How many alphabetic strings are there whose length is at most 5?

Problem 6.5. How many bit strings are there of length at least 4 and at most 6?

Problem 6.6. How many subsets with 4 or more elements does a set of size 30 have?

Problem 6.7. Given a group of ten people, prove that at least 4 are male or at least 7 are female.

Problem 6.8. My family wants to take a group picture. There are 7 men and 5 women, and we want none of the women to stand next to each other. How many different ways are there for us to line up?

Problem 6.9. My family (7 men and 5 women) wants to select a group of 5 of us to plan Christmas. We want at least 1 man and 1 woman in the group. How many ways are there for us to select the members of this group?

Problem 6.10. Compute each of the following: $\binom{8}{4}$, $\binom{9}{9}$, $\binom{7}{3}$, 8!, and 5!

Problem 6.11. For what value(s) of k is $\binom{18}{k}$ largest? smallest?

Problem 6.12. For what value(s) of k is $\binom{19}{k}$ largest? smallest?

Problem 6.13. A computer network consists of 10 computers. Each computer is directly connected to zero or more of the other computers.

(a) Prove that there are at least two computers in the network that are directly connected to the same number of other computers.

(b) Prove that there are an even number of computers that are connected to an odd number of other computers.

Problem 6.14. Simplify the following expression so it does not involve any factorials or binomial coefficients: $\binom{x}{y} / \binom{x+1}{y-1}$

Problem 6.15. Prove that amongst six people in a room there are at least three who know one another, or at least three who do not know one another.

Problem 6.16. Suppose that the letters of the English alphabet are listed in an arbitrary order.

(a) Prove that there must be four consecutive consonants.

(b) Give a list to show that there need not be five consecutive consonants.

(c) Suppose that all the letters are arranged in a circle. Prove that there must be five consecutive consonants.

Problem 6.17. Bob has ten pockets and forty four silver dollars. He wants to put his dollars into his pockets so distributed that each pocket contains a different number of dollars.

(a) Can he do so?

(b) Generalize the problem, considering p pockets and n dollars. Why is the problem most interesting when $n = \dfrac{(p-1)(p-2)}{2}$?

Problem 6.18. Expand and simplify the following.

(a) $(x - 4y)^3$

(b) $(x^3 + y^2)^4$

(c) $(2 + 3x)^6$

(d) $(2i - 3)^5$

(e) $(2i + 3)^4 + (2i - 3)^4$

(f) $(2i + 3)^4 - (2i - 3)^4$

(g) $(\sqrt{3} - \sqrt{2})^3$

(h) $(\sqrt{3} + \sqrt{2})^3 + (\sqrt{3} - \sqrt{2})^3$

(i) $(\sqrt{3} + \sqrt{2})^3 - (\sqrt{3} - \sqrt{2})^3$

Problem 6.19. What is the coefficient of x^6y^9 in $(3x - 2y)^{15}$?

Problem 6.20. What is the coefficient of x^4y^6 in $(x\sqrt{2} - y)^{10}$?

Problem 6.21. Prove Pascal's Identity (Theorem 6.88). (Hint: Just use the definition of the binomial coefficient and do a little algebra.)

Problem 6.22. Prove that for any positive integer n, $\displaystyle\sum_{k=0}^{n}(-2)^k\binom{n}{k} = (-1)^n$. (Hint: *Don't* use induction.)

Problem 6.23. Expand and simplify

$$(\sqrt{1 - x^2} + 1)^7 - (\sqrt{1 - x^2} - 1)^7.$$

Problem 6.24. There are approximately 7,000,000,000 people on the planet. Assume that everyone has a name that consists of exactly k lower-case letters from the English alphabet.

(a) If $k = 8$, is it guaranteed that two people have the same name? Explain.

(b) What is the maximum value of k that would guarantee that at least two people have the same name?

(c) What is the maximum value of k that would guarantee that at least 100 people have the same name?

(d) Now assume that names can be between 1 and k characters long. What is the maximum value of k that would guarantee that at least two people have the same name?

Problem 6.25. Password cracking is the process of determining someone's password, typically using a computer. One way to crack passwords is to perform an exhaustive search that tries every possible string of a given length until it (hopefully) finds it. Assume your computer can test 10,000,000 passwords per second. How long would it take to crack passwords with the following restrictions? Give answers in seconds, minutes, hours, days, or years depending on how large the answer is (e.g. 12,344,440 seconds isn't very helpful). Start by determining how many possible passwords there are in each case.

(a) 8 lower-case alphabetic characters.

(b) 8 alphabetic characters (upper or lower).

(c) 8 alphabetic (upper or lower) and numeric characters.

(d) 8 alphabetic (upper or lower), numeric characters, and special characters (assume there are 32 allowable special characters).

(e) 8 or fewer alphabetic (upper or lower) and numeric characters.

(f) 10 alphabetic (upper or lower), numeric characters, and special characters (assume there are 32 allowable special characters).

(g) 8 characters, with at least one upper-case, one lower-case, one number, and one special character.

Problem 6.26. IP addresses are used to identify computers on a network. In IPv4, IP addresses are 32 bits long. They are usually written using dotted-decimal notation, where the 32 bits are split up into 4 8-bit segments, and each 8-bit segment is represented in decimal. So the IP address 10000001 11000000 00011011 00000100 is represented as 129. 192. 27. 4. The *subnet mask* of a network is a string of k ones followed by $32 - k$ zeros, where the value of k can be different on different networks. For instance, the subnet mask might be 11111111111111111111111100000000, which is 255. 255. 255. 0 in dotted decimal. To determine the *netid*, an IP address is bitwise ANDed with the subnet mask. To determine the *hostid*, an IP address is bitwise ANDed with the bitwise complement of the subnet mask. Since every computer on a network needs to have a different *hostid*, the number of possible *hostid*s determines the maximum number of computers that can be on a network.

Assume that the subnet mask on my computer is currently 255. 255. 255. 0 and my IP address is 209. 140. 209. 27.

(a) What are the *netid* and *hostid* of my computer?

(b) How many computers can be on the network that my computer is on?

(c) In 2010, Hope College's network was not split into subnetworks like it is currently, so all of the computers were on a single network that had a subnet mask of 255. 255. 240. 0. How many computers could be on Hope's network in 2010?

Problem 6.27. Prove that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ by counting the number of binary strings of length n in two ways.

Problem 6.28. In March of every year people fill out brackets for the NCAA Basketball Tournament. They pick the winner of each game in each round. We will assume the tournament starts with 64 teams (it has become a little more complicated than this recently). The first round of the tournament consists of 32 games, the second 16 games, the third 8, the fourth 4, the fifth 2, and the final 1. So the total number of games is $32 + 16 + 8 + 4 + 2 + 1 = 63$. You can arrive at the number of games in a different way. Every game has a loser who is out of the tournament. Since only 1 of the 64 teams remains at the end, there must be 63 losers, so there must be 63 games. Notice that we can also write $1 + 2 + 4 + 8 + 16 + 32 = 63$ as $\sum_{k=0}^{5} 2^k = 2^6 - 1$.

(a) Use a combinatorial proof to show that for any $n > 0$, $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$. (That is, define an appropriate set and count the cardinality of the set in two ways to obtain the identity.)

(b) When you fill out a bracket you are picking who you think the winner will be of each game. How many different ways are there to fill out a bracket? (Hint: If you think about this in the proper way, this is pretty easy.)

(c) If everyone on the planet (7,000,000,000) filled out a bracket, is it guaranteed that two people will have the same bracket? Explain.

(d) Assume that everyone on the planet fills out k different brackets and that no brackets are repeated (either by an individual or by anybody else). How large would k have to be before it is guaranteed that somebody has a bracket that correctly predicts the winner of every game?

(e) Assume every pair of people on the planet gets together to fill out a bracket (so everyone has 6,999,999 brackets, one with every other person on the planet). What is the smallest and largest number of possible repeated brackets?

Problem 6.29. Mega Millions has 56 white balls, numbered 1 through 56, and 46 red balls, numbered 1 through 46. To play you pick 5 numbers between 1 and 56 (corresponding to white balls) and 1 number between 1 and 46 (corresponding to a red ball). Then 5 of the 56 balls and 1 of the 46 balls are drawn randomly (or so they would have us believe). You win if your numbers match all 6 balls.

(a) How many different draws are possible?

(b) If everyone in the U.S.A. bought a ticket (about 314,000,000), is it guaranteed that two people have the same numbers? Three people?

(c) If everyone in the U.S.A. bought a ticket, what is the maximum number of people that are guaranteed to share the jackpot?

(d) Which is more likely: Winning Mega Millions or picking every winner in the NCAA Basketball Tournament (see previous question)? How many more times likely is one than the other?

(e) I purchased a ticket last week and was surprised when *none* of my six numbers matched. Should I have been surprised? What are the chances that a randomly selected ticket will match none of the numbers?

(f) (hard) What is the largest value of k such that you are more likely to pick at least k winners in the NCAA Basketball Tournament than you are to win Mega Millions?

Problem 6.30. You get a new job and your boss gives you 2 choices for your salary. You can either make \$100 per day or you can start at \$.01 on the first day and have your salary doubled every day. You know that you will work for k days. For what values of k should you take the first offer and for which should you take the second offer? Explain.

Problem 6.31. The 300-level courses in the CS department are split into three groups: Foundations (361, 385), Applications (321, 342, 392), and Systems (335, 354, 376). In order to get a BS in computer science at Hope you need to take at least one course from each group.

(a) How many different ways are there of satisfying this requirement by taking exactly 3 courses?

(b) If you take four 300-level courses, how many different possibilities do you have that satisfy the requirements?

(c) How many total ways are there to take 300-level courses that satisfy the requirements?

(d) What is the smallest k such that no matter which k 300-level courses you choose, it is guaranteed that you will satisfy the requirement?

Problem 6.32. Let $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Prove that $A^n = \begin{bmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix}$.

Chapter 7: Graph Theory

In this chapter we will provide a *very brief* and *very selective* introduction to graphs. Graph theory is a very wide field and there are many thick textbooks on the subject. The main point of this chapter is to provide you with the basic notion of what a graph is, some of the terminology used, a few applications, and a few interesting and/or important results.

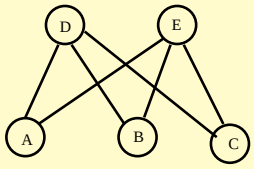
7.1 Types of Graphs

Definition 7.1. *A* **(simple) graph** $G = (V, E)$ *consists of*

- V*, a nonempty set of* **vertices** *and*
- E*, a set of* unordered pairs *of distinct vertices called* **edges**.

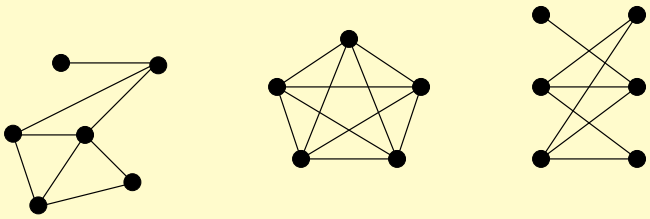
The **order** *of a graph is* $|V|$*, the number of vertices.*

Example 7.2. Here is an example of a graph with the set of vertices and edges listed on the right. Vertices are usually represented by means of dots on the plane, and the edges by means of lines connecting these dots.



V={A,B,C,D,E}
E={ (A,D),(A,E),(B,D),
(B,E),(C,D),(C,E)}

Example 7.3. Sometimes we just care about the visual representation of a graph. Here are three examples.



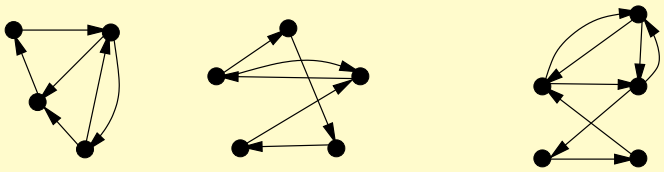
There are several variations of graphs. We will provide definitions and examples of the most common ones.

Definition 7.4. *A* **directed graph** *(or* **digraph***)* $G = (V, E)$ *consists of*

- V*, a nonempty set of* **vertices** *and*
- E*, a set of* ordered pairs *of distinct vertices called* **directed edges** *(or just* **edges***).*

The **order** *of a digraph is* $|V|$*, the number of vertices.*

Example 7.5. Here are three examples of directed graphs.



As you would probably suspect, the only difference between simple graphs and directed graphs is that the edges in directed graphs have a direction. We should note that simple graphs are sometimes called **undirected graphs** to make it clear that the graphs are not directed.

Example 7.6. In a simple graph, $\{u, v\}$ and $\{v, u\}$ are just two different ways of talking about the same edge–the edge between u and v. In a directed graph, (u, v) is the edge from u to v and (v, u) is the edge from v to u. These are not the same, and they may or may not both be present.

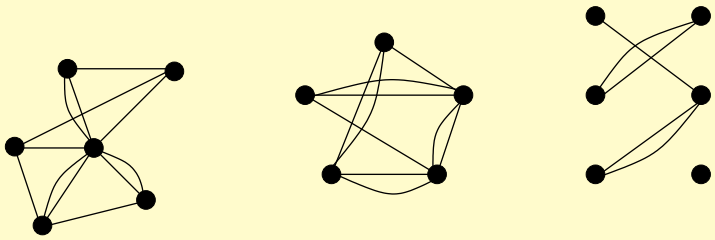
Definition 7.7. *A* **multigraph (directed multigraph)** $G = (V, E)$ *consists of*

- V*, a set of vertices,*
- E*, a set of edges, and*
- *a function* f *from* E *to* $\{\{u, v\} : u \neq v \in V\}$
  (function f *from* E *to* $\{(u, v) : u \neq v \in V\}$*.)*

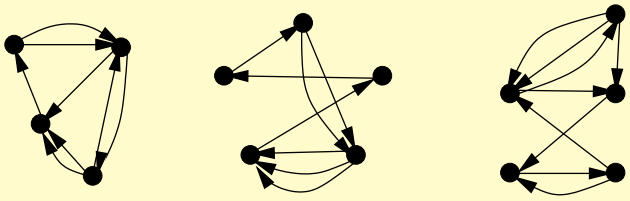
Two edges e_1 *and* e_2 *with* $f(e_1) = f(e_2)$ *are called* **multiple edges**.

Although the definition looks a bit complicated, a **multigraph** $G = (V, E)$ is just a graph in which multiple edges are allowed between a pair of vertices.

Example 7.8. Here are a few examples of multigraphs.

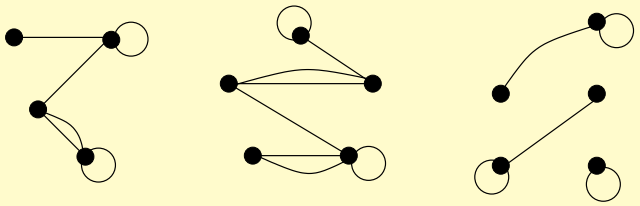


Here are some examples of directed multigraphs.

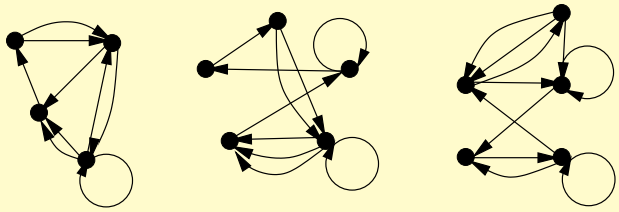


Definition 7.9. *A* **pseudograph** $G = (V, E)$ *is a graph in which we allow* **loops***–that is, edges from a vertex to itself. As you might imagine, a* **pseudo-multigraph** *allows both loops and multiple edges.*

Example 7.10. Here are some pseudographs.



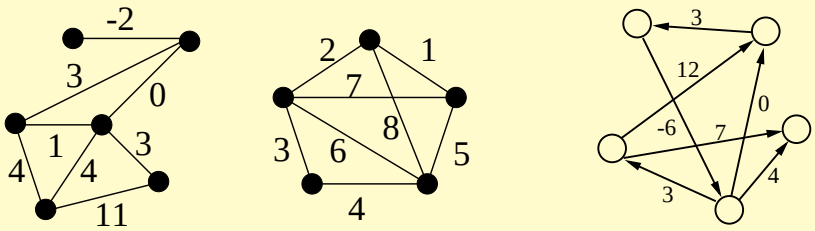
Here are a few directed pseudographs.



Definition 7.11. *A* **weighted graph** *is a graph (or digraph) with the additional property that each edge e has associated with it a real number $w(e)$ called its* weight*.*

A **weighted digraph** *is often called a* **network***.*

Example 7.12. Here are two examples of weighted graphs and one weighted directed graph.



As we have seen, there are several ways of categorizing graphs:

- Directed or undirected edges.
- Weighted or unweighted edges.
- Allow multiple edges or not.
- Allow loops or not.

Unless specified, you can usually assume a graph does not allow multiple edges or loops since these aren't that common. Generally speaking, you can assume that if a graph is not specified as weighted or directed, it isn't. The most common graphs we'll use are graphs, digraphs, weighted graphs, and networks.

Note: *When writing graph algorithms, it is important to know what characteristics the graphs have. For instance, if a graph might have loops, the algorithm should be able to handle it. Some algorithms do not work if a graph has loops and/or multiple edges, and some only apply to directed (or undirected) graphs.*

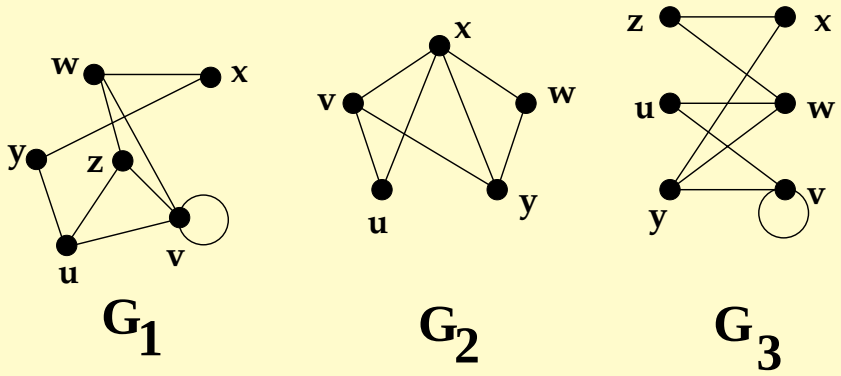
7.2 Graph Terminology

Definition 7.13. *Given a graph $G = (V, E)$, we denote the number of vertices in G by $|V|$ and the number of edges by $|E|$ (a notation that makes perfect sense since V and E are sets).*

Definition 7.14. *Let u and v be vertices and $e = \{u, v\}$ be an edge in undirected graph G.*

- *The vertices u and v are said to be* **adjacent**
- *The vertices u and v are called the* **endpoints** *of the edge e.*
- *The edge e is said to be* **incident with** *u and v.*
- *The edge e is said to* **connect** *u and v.*
- *The* **degree** *of a vertex, denoted $deg(v)$, is the number of edges incident with it.*

Example 7.15. Consider the following graphs.



In graph G_1, we can say:

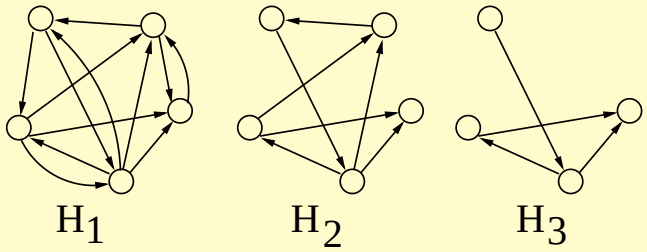
- w is adjacent to x.
- w and x are the endpoints of the edge (w, x).
- (w, x) is incident with both w and x.
- (w, x) connects vertices w and x.

The following table gives the degree of each of the vertices in the graphs above.

G_1	G_2	G_3
deg(u)=3	deg(u)=2	deg(u)=2
deg(v)=5	deg(v)=3	deg(v)=4
deg(w)=3	deg(w)=2	deg(w)=3
deg(x)=2	deg(x)=4	deg(x)=2
deg(y)=2	deg(y)=3	deg(y)=3
deg(z)=3		deg(z)=2

Definition 7.16. *A* **subgraph** *of a graph $G = (V, E)$ is a graph $G' = (V', E')$ such that $V' \subset V$ and $E' \subset E$.*

Example 7.17. Consider the following three graphs:



Notice that H_2 is a subgraph of H_1 and that H_3 is a subgraph of both H_1 and H_2.

Definition 7.18. *A $u-v$* **walk** *is an alternating sequence of vertices and edges in G with starting vertex u and ending vertex v such that every edge joins the vertices immediately preceding it and immediately following it.*

You can think of a walk as follows: Put your pencil down on a vertex and trace around edges however you like until you reach some destination vertex. You are allowed to repeat edges and vertices as often as you like–just like you may repeat sidewalks and paths when you go for a walk (thus the name).

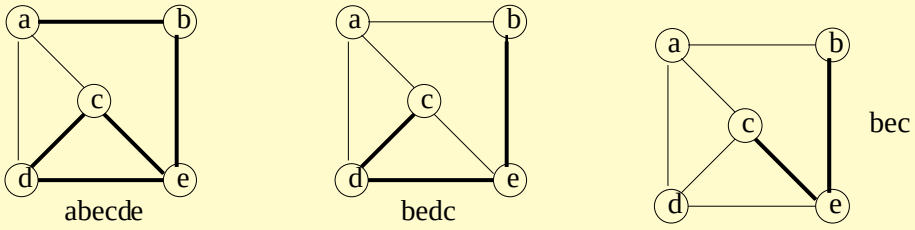
Definition 7.19. *A $u-v$* **trail** *is a $u-v$ walk that does not repeat an edge.*

Notice that a trail *may* repeat a vertex.

Definition 7.20. *A $u-v$* **path** *is a walk that does not repeat any vertex.*

It should be relatively easy to see that paths cannot repeat an edge (because to repeat an edge you have to repeat a vertex).

Example 7.21. In the first graph, the trail *abecde* is indicated with the dark lines. It is not a path since it repeats the vertex e. The second and third graphs show examples of paths.



Although not drawn (because it is harder to represent clearly on a drawing), *acdecabecdeba* is an example of a walk[a] To confirm it, you just need to verify that there is an edge between adjacent vertices on the list. On the other hand, *abcde* is *not* a path, trail, or walk because (b, c) is not an edge.

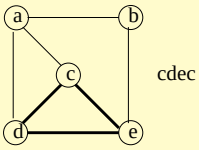
[a]This walk is specified by just the vertices and not both the vertices and edges as in the definition. If multiple edges are not allowed (i.e. we are not working with a multigraph), then there is no need to list the edges since they are clear.

Definition 7.22. *A* **cycle** *(or* **simple cycle***) is a list of vertices $v_1, v_2, \ldots, v_k$, with no repeats such that (v_i, v_{i+1}) is an edge for $i = 1, \ldots, k-1$, and (v_k, v_1) is an edge.*

Put another way, a cycle is a path to which we append an edge from the last to the first vertex.

The number of vertices in a cycle is called its **length**.

Example 7.23. Here is a graph with a cycle of length 3.



★**Exercise 7.24.** Find a cycle of length 4 and a cycle of length 5 in the graph from Example 7.23. Is there a cycle of length 6? Explain why or why not.

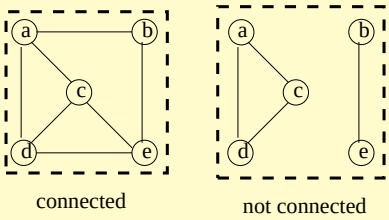
Answer _____

_____

Definition 7.25. *A graph is called* **connected** *if there is a path between every pair of distinct vertices.*

A **connected component** *of a graph is a maximal connected subgraph.*

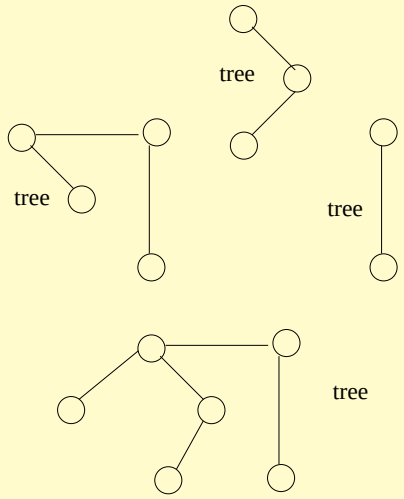
Example 7.26. Below are two graphs, each drawn inside dashed boxes. The graph on the left is connected. The one on the right is not connected. It has two connected components.



★**Exercise 7.27.** Draw a graph that has two connected components, one that is a cycle of length 4 and one that is a cycle of length 3.

Definition 7.28.
- *A* **tree** *(or* **unrooted tree***) is a connected acyclic graph. That is, a graph with no cycles.*
- *A vertex of degree one in a tree is called a* **leaf***.*
- *A* **forest** *is a collection of trees.*

Example 7.29. Here are four trees. If they were all part of the same graph, we could consider the graph a forest.



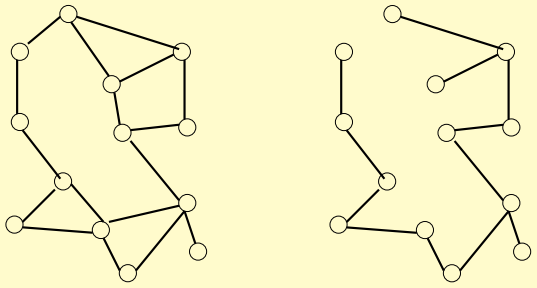
★**Exercise 7.30.** Draw a tree that has 5 vertices, one vertex with degree 4 and the others with degree 1.

★**Exercise 7.31.** Draw a forest with 5 trees that has 6 vertices.

Note: *These trees are not to be confused with* rooted trees *(e.g.* binary trees*). When computer scientists use the term* tree*, they usually mean rooted trees, not the trees we are discussing here. When you see/hear the term 'tree,' it is important to be clear about which one the writer/speaker has in mind.*

Definition 7.32. *A* **spanning tree** *of G is a subgraph which is a tree and contains all of the vertices of G.*

Example 7.33. Below is a graph (on the left) and one of several possible spanning trees (on the right).



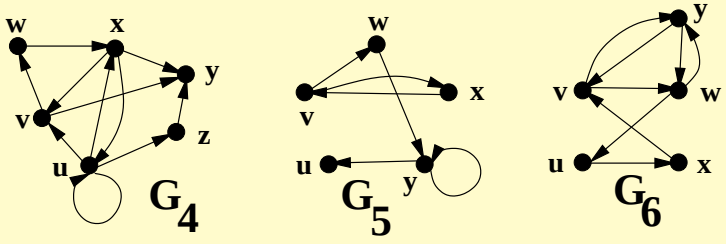
G spanning tree of G

Here is some terminology related to directed graphs.

Definition 7.34. *Let u, v be vertices in a directed graph G, and $e = (u, v)$ be an edge in G.*

- *u is said to be* **adjacent to** *v.*
- *v is said to be* **adjacent from** *u.*
- *u is called the* **initial vertex** *of (u, v).*
- *v is called the* **terminal** *or* **end vertex** *of (u, v).*
- *The* **in-degree** *of u, denoted by $deg^-(u)$, is the number of edges in G which have u as their terminal vertex.*
- *The* **out-degree** *of u, denoted by $deg^+(u)$, is the number of edges in G which have u as their initial vertex.*

Example 7.35. Consider the three graphs below.



Consider the edge (w, x) in G_4.

- w is adjacent to x and x is adjacent from w.
- w is the initial vertex and x is the terminal vertex of the edge (w, x).

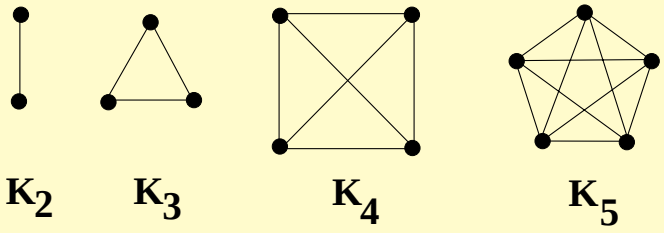
This table gives the in-degree and out-degree for the vertices in graphs G_4, G_5, and G_6.

G_4		G_5		G_6	
$\deg^-$(u)=2	$\deg^+$(u)=4	$\deg^-$(u)=1	$\deg^+$(u)=0	$\deg^-$(u)=1	$\deg^+$(u)=1
$\deg^-$(v)=2	$\deg^+$(v)=2	$\deg^-$(v)=1	$\deg^+$(v)=2	$\deg^-$(v)=2	$\deg^+$(v)=2
$\deg^-$(w)=1	$\deg^+$(w)=1	$\deg^-$(w)=1	$\deg^+$(w)=1	$\deg^-$(w)=2	$\deg^+$(w)=2
$\deg^-$(x)=2	$\deg^+$(x)=3	$\deg^-$(x)=1	$\deg^+$(x)=1	$\deg^-$(x)=1	$\deg^+$(x)=1
$\deg^-$(y)=3	$\deg^+$(y)=0	$\deg^-$(y)=2	$\deg^+$(y)=2	$\deg^-$(y)=2	$\deg^+$(y)=2
$\deg^-$(z)=1	$\deg^+$(z)=1				

7.3 Some Special Graphs

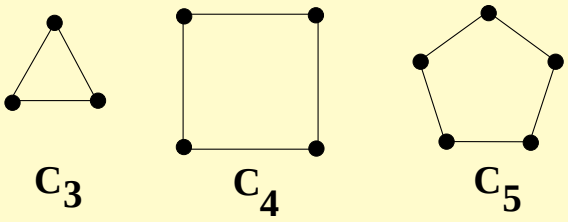
Definition 7.36. *The* **complete graph** *with n vertices K_n is the graph where every pair of vertices is adjacent. Thus, K_n has $\binom{n}{2}$ edges.*

Example 7.37. Here are the complete graphs with $n = 2, 3, 4, 5$.



Definition 7.38. *C_n denotes a* **cycle** *of length n. It is a graph with n edges, and n vertices $v_1, \ldots, v_n$, where v_i is adjacent to v_{i+1} for $n = 1, \ldots, n-1$, and v_1 is adjacent to v_n.*

Example 7.39. Here are the cycles of length 3, 4, and 5.



Definition 7.40. *P_n denotes a* path *of length n. It is a graph with n edges, and $n+1$ vertices $v_0, v_1, \ldots, v_n$, where v_i is adjacent to v_{i+1} for $n = 0, 1, \ldots, n-1$.*

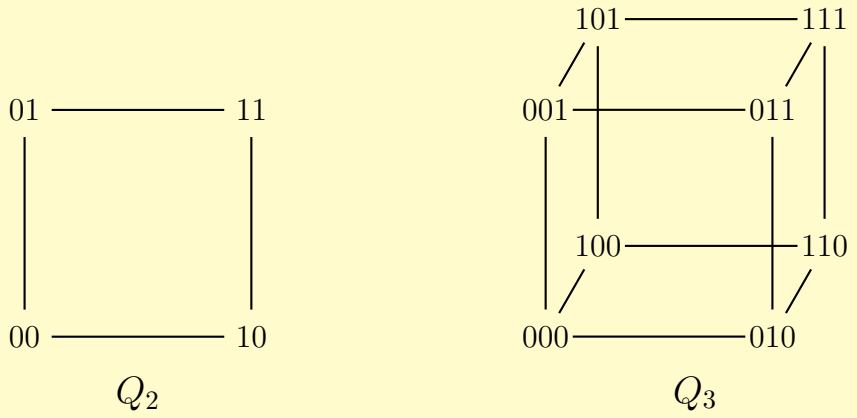
We won't provide an example of the paths because they are pretty easy to visualize. For instance, P_3 is simply C_4 with one edge removed.

Definition 7.41. *Q_n denotes the n-dimensional* **cube** *(or* **hypercube***). There are two equivalent ways to define Q_n.*

- *Q_1 is the graph consisting of a single vertex, and Q_n is constructed by taking two copies of Q_{n-1} and connecting corresponding vertices between the two copies. Hopefully you can see that this leads to $Q_2 = P_2$ and $Q_3 = C_4$.*
- *Q_n is the graph with 2^n vertices numbered 0 through $2^n - 1$ where two vertices are connected if the binary representation of their numbers differs in exactly one place.*

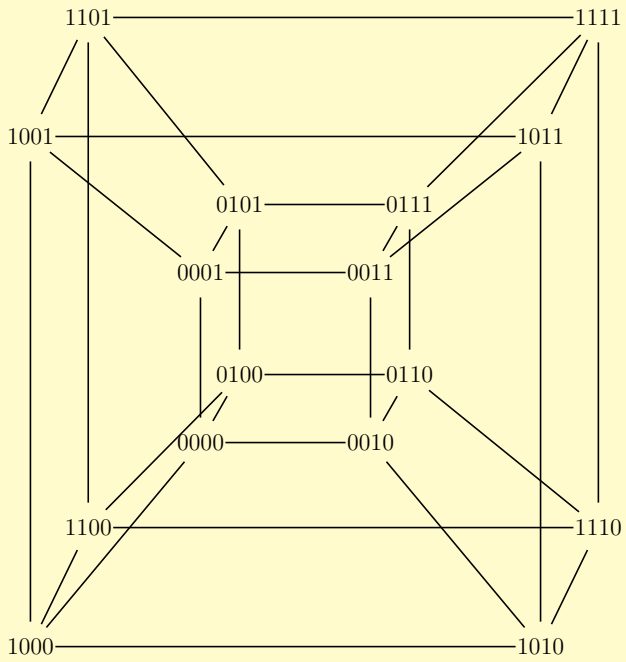
It is not difficult to determine that Q_n has $n2^{n-1}$ edges.

Example 7.42. Here are Q_2 and Q_3, with vertices labeled as mentioned in the definition.



Q_2 $\qquad\qquad$ Q_3

Notice that in Q_2, the vertex labeled 11 is adjacent to the vertices labeled 10 and 01 since each of these differ in one bit. Similarly, the vertex labeled 101 in Q_3 is adjacent to the vertices labeled 001, 111, and 100 for the same reason. Next is Q_4, also labeled according to the definition.



Q_4

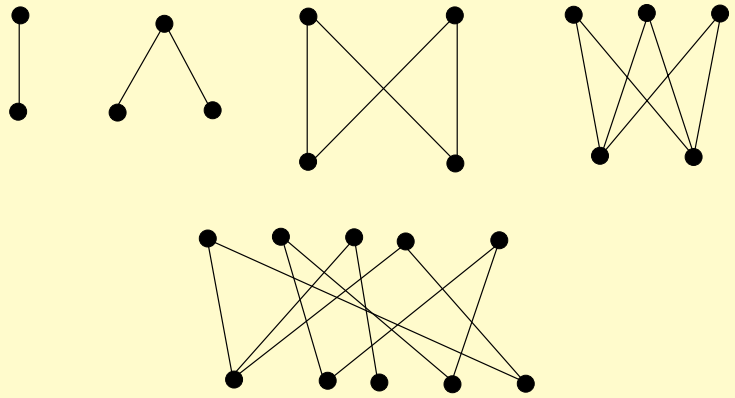
It should not be too difficult to see that Q_1 is the same as P_1 which is the same as K_2.

Definition 7.43. *A simple graph G is called* **bipartite** *if the vertex set V can be partitioned into two disjoint nonempty sets V_1 and V_2 such that every edge connects a vertex in V_1 to a vertex in V_2.*

Put another way, no vertices in V_1 are connected to each other, and no vertices in V_2 are connected to each other.

Although there may be different ways of assigning the vertices to V_1 and V_2, it does not matter. If there is at least one way to do so such that all edges go between V_1 and V_2, then G is bipartite.

Example 7.44. Here are a few bipartite graphs.



Notice that although these are drawn to make it clear what the partition is (i.e. V_1 is the top row of vertices and V_2 is the bottom row), a graph does not have to be drawn as such in order to be bipartite. They are often drawn this way out of convenience. For instance, the hypercubes are all bipartite even though they are not drawn this way.

Definition 7.45. *$K_{m,n}$ denotes the* **complete bipartite graph** *with $m+n$ vertices. That is, it is the graph with $m+n$ vertices that is partitioned into two sets, one of size n and the other of size m, such that every possible edge between the two sets is in the graph.*

Example 7.46. The first four graphs from Example 7.44 are complete bipartite graphs. The first is $K_{1,1}$, the second is $K_{1,2}$ (or $K_{2,1}$), the third is $K_{2,2}$, and the fourth is $K_{3,2}$ (or $K_{2,3}$).

★**Exercise 7.47.** Which of the following graphs are bipartite? Briefly justify your answers.

(a) C_4. _____

(b) C_5. _____

(c) K_4. _____

(d) Q_3. _____

(e) P_n for any $n > 0$. _____

★**Question 7.48.** Prove or disprove: Every tree with at least 2 vertices is bipartite. (Hint: You can prove this by induction on the number of nodes.)

7.4 Handshaking Lemma

The following theorem is valid not only for simple graphs, but also for multigraphs and pseudographs.

Theorem 7.49 (Handshake Lemma)**.** *Let $G = (V, E)$ be a graph. Then*

$$\sum_{v \in V} \deg(v) = 2|E|.$$

Proof: *Let $X = \{(e, v) : e \in E, v \in V,$ and e and v are incident$\}$. We will compute $|X|$ in two ways. Each edge $e \in E$ is incident with exactly 2 vertices. Thus,*

$$|X| = 2|E|.$$

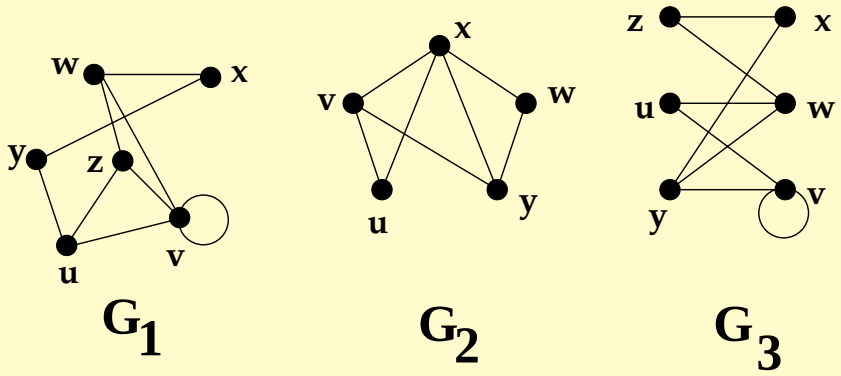
Also, each vertex $v \in V$ is incident with $deg(v)$ edges. Thus, we have that

$$|X| = \sum_{v \in V} deg(v).$$

Setting these equal, we have the result. □

The proof in the previous theorem is an example of a combinatorial proof. It is a neat technique where you prove a formula by counting the number of objects in a set in two different ways.

Example 7.50. Consider the following graphs.



A quick tabulation of the degrees of the vertices and the number of edges reveals the following:

Graph	G_1	G_2	G_3
$\|E\|$	9	7	8
$\sum_{v \in V} deg(v)$	18	14	16

These results are certainly consistent with Theorem 7.49.

Undirected graphs have an interesting property that is really easy to prove using Theorem 7.49.

Corollary 7.51. *Every graph has an even number of vertices of odd degree.*

Proof: *The sum of an odd number of odd numbers is odd. Since the sum of the degrees of the vertices in a simple graph is always even, one cannot have an odd number of odd degree vertices.* □

The situation is slightly different, but not too surprising, for directed graphs.

Theorem 7.52. *Let $G = (V, E)$ be a directed graph. Then*

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|.$$

We won't provide a proof of this theorem (it's almost obvious), but you should verify it for the graphs in Example 7.35 by adding up the degrees in each column and comparing the appropriate sums.

7.5 Graph Representation

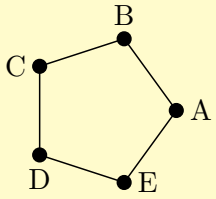
We provide only a very brief discussion of graph representation. Consult your favorite data structure book for more details.

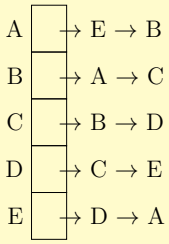
Let $G = (V, E)$ be a graph with n vertices and m edges. That is, $|V| = n$, and $|E| = m$. There are two common ways of representing G. (There is actually a third, but it isn't nearly as common as the two we will discuss.)

The first method stores, for each vertex, a list of all of the vertices it is adjacent to.

Definition 7.53. *The* **adjacency list** *representation of a graph maintains, for each vertex, a list of all of the vertices adjacent to that vertex. This can be implemented in many ways, but often an array of linked lists is used.*

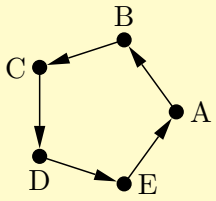
Example 7.54. A drawing of C_5 is given below on the left. An adjacency list representation is given below on the right.

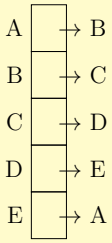




Notice that every edge is represented twice. For instance, the edge (A, B) means that A and B are connected to each other. Thus, B is on A's list, and A is on B's list.

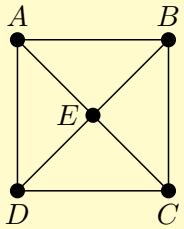
Example 7.55. A drawing of a directed cycle of length 5 is given below on the left. An adjacency list representation is given next to it.

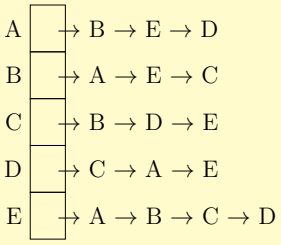




Notice that this is a lot like the previous example except that each list only has one element on it. That is because (A, B) is an edge (for instance), but (B, A) is not an edge. So B is on A's list, but A is not on B's list.

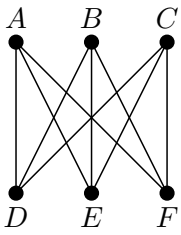
Example 7.56. Here is another example of a graph on the left with the adjacency list representation on the right.

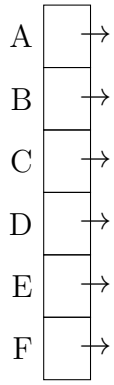




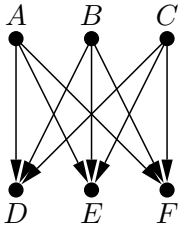
Note that the order the vertices are listed does not matter.

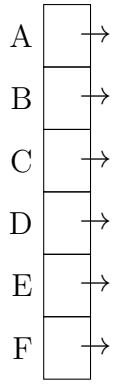
★**Exercise 7.57.** Give the adjacency list representation for $K_{3,3}$ as drawn below.





★**Exercise 7.58.** Give the adjacency list representation for the directed graph similar to $K_{3,3}$ drawn below.





The graph in Example 7.56 has 5 vertices and 8 edges (so $n = 5$ and $m = 8$). The adjacency list uses an array of size 5 and there are 5 linked lists that contain a total of $3+3+3+3+4 = 16 = 2*8$ nodes. Notice that this is twice the number of edges because each edge is stored twice (because if (u, v) is an edge, u is stored on v's list and v is stored on u's list). For each node we need to store the *value* and the *next* node, so the linked lists take up about $2(2 * 8) = 4 * 8 = 4m$ memory. Since the array takes about $5 = n$ memory, the memory requirement for an adjacency list representation of the graph is approximately $n + 4m = \Theta(n + m)$.

Notice that the discussion in the previous paragraph generalizes to all graphs. That is, the space requirement for the adjacency list representation of a graph is approximately $n + 4m = \Theta(n + m)$.

Hopefully it is not too difficult to see that for directed graphs, the amount of memory required is about $n + 2m = \Theta(n + m)$ because each edge is only stored once.

For weighted graphs, an additional field can be stored in each node for the weight of each edge. So for undirected weighted graphs, the memory requirement goes up to about $n + 6m$, and for directed weighted graphs it is about $n + 3m$. In both cases, it is still $\Theta(n + m)$.

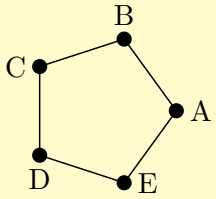
The second method of storing a graph makes it so you can ask directly "Is (u, v) and edge?" This is accomplished by storing a matrix whose rows and columns are indexed by the vertices.

Definition 7.59. *The* **adjacency matrix** M *of a graph* G *is the* n *by* n *matrix* M *defined as*

$$M(i,j) = \begin{cases} 1 & \text{if } (i,j) \text{ is an edge} \\ 0 & \text{if } (i,j) \text{ is not an edge} \end{cases}$$

We often assume that the vertices are numbered $0, 1, \ldots, n-1$ since that is how we typically index matrices. In the next few examples we will continue with our examples with vertices labeled A, B, etc. To make the interpretation of the matrices clear, we label the rows and columns. You can also just think of a mapping of A to 0, B to 1, etc.

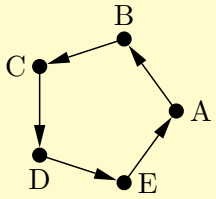
Example 7.60. A drawing of C_5 is given below on the left, the adjacency list in the middle, and the adjacency matrix on the right.



A → E → B
B → A → C
C → B → D
D → C → E
E → D → A

	A	B	C	D	E
A	0	1	0	0	1
B	1	0	1	0	0
C	0	1	0	1	0
D	0	0	1	0	1
E	1	0	0	1	0

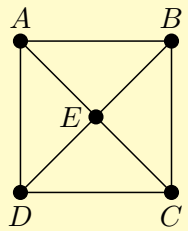
Example 7.61. A drawing of a directed cycle of length 5 is given below on the left. An adjacency list representation is given in the middle and the adjacency matrix on the right.



A → B
B → C
C → D
D → E
E → A

	A	B	C	D	E
A	0	1	0	0	0
B	0	0	1	0	0
C	0	0	0	1	0
D	0	0	0	0	1
E	1	0	0	0	0

Example 7.62. Here is another example of a graph on the left, the adjacency list representation on the center, and the adjacency matrix on the right.



A → B → E → D
B → A → E → C
C → B → D → E
D → C → A → E
E → A → B → C → D

	A	B	C	D	E
A	0	1	0	1	1
B	1	0	1	0	1
C	0	1	0	1	1
D	1	0	1	0	1
E	1	1	1	1	1

Note: *You may or may not have noticed from these examples that the adjacency matrix of an undirected graph is always symmetric. If you think about it, the reason should be obvious.*

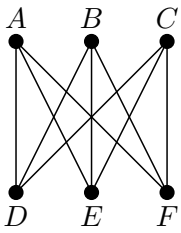
The same cannot be said of directed graphs, as should be obvious from Example 7.61.

From these examples, it should be relatively clear that the amount of space needed to store an adjacency matrix with n vertices and m edges is about $n^2 = \Theta(n^2)$. Notice that it does not depend on m, since a larger m just means more 1s and fewer 0s in the matrix.

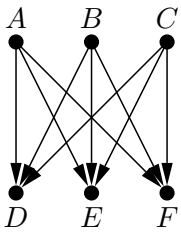
If G is weighted, we can store the weights in the matrix instead of just 0 or 1. For non-adjacent vertices, we store ∞, or *MAX_INT* (or -1 if only positive weights are valid). If done this way, the space requirement remains $n^2 = \Theta(n^2)$. Alternatively, a second matrix can be used to store the weights, doubling the space requirement, which is still $\Theta(n^2)$.

Notice the amont of space required to store both directed and undirected graphs is the same with the adjacency matrix.

★**Exercise 7.63.** Give the adjacency matrix representation for $K_{3,3}$ as drawn below.



★**Exercise 7.64.** Give the adjacency matrix representation for the directed graph similar to $K_{3,3}$ drawn below.



Obviously, how much space is required to store a graph is of importance, but so is how much time is required to do basic operations on a graph. For instance, the most common things one might want to do on a graph are determine whether or not two vertices are adjacent and iterate over the edges that are incident with a vertex (put another way, iterate over all of the neighbors of a vertex). For a weighted graph, one would probably ask the weight of an edge somewhat often. There are certainly other important operations one might want to perform on a graph. Since you have all of the tools you need to answer such questions, we will ask you to explore them at the end of the chapter.

So which representation is better? We will also let you think about that at the end of the chapter, but hopefully it is somewhat clear that answering that question requires you to consider both time and space requirements.

7.6 Problem Solving with Graphs

There are many problems on graphs that are of interest for various reasons. The following very short list contains some of the more common ones.

- Path: Is there a path from A to B?
- Cycles: Does the graph contain a cycle?
- Connectivity: Is there a way to get between any two vertices in the graph?
- Biconnectivity: Will the graph become disconnected if one vertex is removed?
- Planarity: Is there a way to draw the graph without edges crossing?
- Shortest Path: What is the shortest path from A to B? (weighted and unweighted versions)
- Longest Path: What is the longest path from A to B? (weighted and unweighted versions)
- Minimum Spanning Tree: What is the "most efficient" way to connect the vertices (weighted graphs)?
- Traversability: Is is possible to travel to every vertex without repeating a vertex? Is it possible to travel over every edge without repeating an edge?
- Traveling Salesman: What is the shortest route that visits every vertex and returns to the starting vertex? (weighted graphs)

Knowing what graph problems have been studied and what is known about each is very important. Many problems can be modeled using graphs, and once a problem has been mapped to a particular graph problem, it can be helpful to know the best way to solve it.

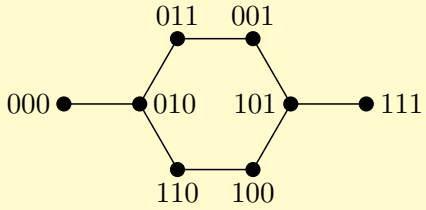
We finish the chapter by giving several examples of problems whose solutions become simpler when using a graph-theoretic model as well as develop some new graph terminology. It is important to mention that whole books are written just about graph theory, and even they have to pick a small subset of the topic. Thus, what is presented in the remainder of this chapter should not be interpreted in any way to be the most important topics in graph theory. It is just a very small selection of easy to understand topics that are related to interesting problems. Dozens–maybe even hundreds–of other topics could have been chosen. It should be noted that the author has even resisted the urge to include one of his favorite graph topics, *graph pebbling*, even though it is a somewhat interesting topic. Well, to him anyway.

7.6.1 Sample Problems

Example 7.65. A wolf, a goat, and a cabbage are on one bank of a river. The ferryman wants to take them across, but his boat is too small to accommodate more than one of them at a time. He cannot leave the wolf and the goat together (the wolf will eat the goat), or the cabbage and the goat (the goat will eat the cabbage) unless he is with them. Can the ferryman still get all of them across the river?

Solution: Represent the position of a single item by 0 for one bank of the river and 1 for the other bank. The position of the three items can now be given as an ordered triplet, say (W, G, C). For example, $(0, 0, 0)$ means that the three items are on one bank of the river, $(1, 0, 0)$ means that the wolf is on one bank of the river while the goat and the cabbage are on the other bank. The object of the puzzle is now seen to be to move from $(0, 0, 0)$ to $(1, 1, 1)$ by traversing certain edges of Q_3 while avoiding other edges. Note that Q_3 is the correct set of edges to consider since he can only move one of the three items at a time.

But there are some edges he cannot use. For instance, $000 \to 100$ is illegal since it would mean he takes the wolf to the other side, leaving the goat and cabbage together. Similarly, $000 \to 001$ is illegal. Thus, from 000, the only choice is to go to 010. Continuing this analysis, it can be determined that the set of legal edges is as in the following graph:



Based on this, one answer is $000 \to 010 \to 011 \to 001 \to 101 \to 111$. This means that the ferryman (i) takes the goat across, (ii) returns and takes the cabbage over, (iii) brings back the goat, (iv) takes the wolf over, (v) returns and takes the goat over.

Another answer is $000 \to 010 \to 110 \to 100 \to 101 \to 111$. This means that the ferryman (i) takes the goat across, (ii) returns and takes the wolf over, (iii) brings back the goat, (iv) takes the cabbage over, (v) returns and takes the goat over.

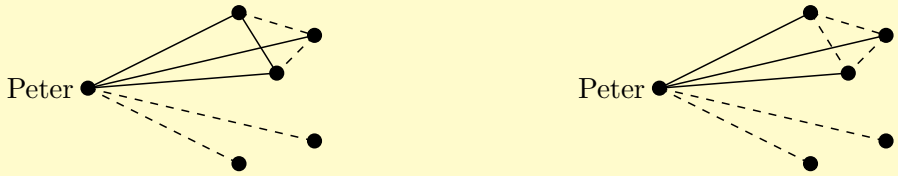
Go to https://xkcd.com/1134/ to see a funny, but incorrect, solution.

Example 7.66. Prove that amongst six people in a room there are at least three who know one another, or at least three who do not know one another.

Solution: Consider an arbitrary person of this group (call him Peter). There are five other people, and of these, either three of them know Peter or else, three of them do not know Peter.

Let us assume three know Peter. If two of these three people know one another, then we have a triangle of three people who know each other (Peter and these

two–see the graph below on the left, where the acquaintances are marked by solid lines). If no two of these three people know one another, then we have three mutual strangers (see the graph on the right).



The argument for the case when three do not know Peter is similar and is left to the reader.

Example 7.67. Mr. and Mrs. Landau invite four other married couples for dinner. Some people shook hands with some others, and the following rules were noted: (i) a person did not shake hands with himself, (ii) no one shook hands with his spouse, (iii) no one shook hands more than once with the same person. After the introductions, Mr. Landau asks the nine people how many hands they shook. Each of the nine people asked gives a different number. How many hands did Mrs. Landau shake?

Solution: The given numbers can either be $0, 1, 2, \ldots, 8$, or $1, 2, \ldots, 9$. Now, the sequence $1, 2, \ldots, 9$ must be ruled out, since if a person shook hands nine times, then he must have shaken hands with his spouse, which is not allowed. The only permissible sequence is thus $0, 1, 2, \ldots, 8$. Consider the person who shook hands 8 times, as in figure 7.1. Discounting himself and his spouse, he must have shaken hands with everybody else. This means that he is married to the person who shook 0 hands! We now consider the person that shook 7 hands, as in figure 7.2. He didn't shake hands with himself, his spouse, or with the person that shook 0 hands. But the person that shook hands only once did so with the person shaking 8 hands. Thus the person that shook hands 7 times is married to the person that shook hands once. Continuing this argument, we see the following pairs: $(8, 0)$, $(7, 1)$, $(6, 2)$, $(5, 3)$. This leaves the person that shook hands 4 times without a partner, meaning that this person's partner did not give a number, hence this person must be Mrs. Landau! Conclusion: Mrs. Landau shook hands four times. A graph of the situation appears in figure 7.3.

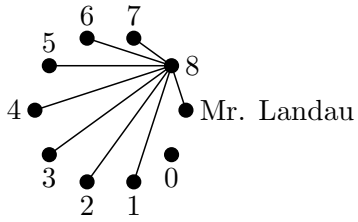


Figure 7.1: Example 7.67.

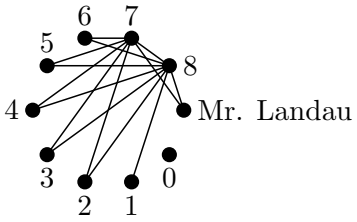


Figure 7.2: Example 7.67.

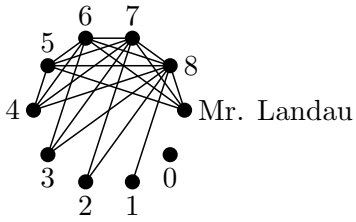


Figure 7.3: Example 7.67.

7.6.2 Trails, Paths, and Cycles

Definition 7.68. *Recall that a* **trail** *is a walk where all the edges are distinct. An* **Eulerian trail** *on a graph Gis a trail that traverses every edge of G. A* **tour** *of G is a closed walk that traverses each edge of G at least once. An* **Euler tour** *(or* **Euler cycle***) on G is a tour traversing each edge of G exactly once, that is, a closed Euler trail. A graph is* **Eulerian** *if it contains an Euler tour.*

It turns out there is a very easy way to determine whether or not a graph has an Euler tour.

Theorem 7.69. *A nonempty connected graph is Eulerian if and only if it has no vertices of odd degree.*

Proof: *Assume first that G is Eulerian, and let C be an Euler tour of G starting and ending at vertex u. Each time a vertex v is encountered along C, two of the edges incident to v are accounted for. Since C contains every edge of G, $d(v)$ is then even for all $v \neq u$. Also, since C begins and ends in u, $d(u)$ must also be even.*

Conversely, assume that G is a connected nonEulerian graph with at least one edge and no vertices of odd degree. Let W be the longest walk in G that traverses every edge at most once:

$$W = v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{n-1}, v_{n-1}v_n, v_n.$$

Then W must traverse every edge incident to v_n, otherwise, W could be extended into a longer walk. In particular, W traverses two of these edges each time it passes through v_n and traverses $v_{n-1}v_n$ at the end of the walk. This accounts for an odd number of edges, but the degree of v_n is even by assumption. Hence, W must also begin at v_n, that is, $v_0 = v_n$. If W were not an Euler tour, we could find an edge not in W but incident to some vertex in W since G is connected. Call this edge uv_i. But then we can construct a longer walk:

$$u, uv_i, v_i, v_iv_{i+1}, \ldots, v_{n-1}v_n, v_n, v_0v_1, \ldots, v_{i-1}v_i, v_i.$$

This contradicts the definition of W, so W must be an Euler tour. □

The following problem is perhaps the originator of graph theory.

Example 7.70 (Königsberg Bridge Problem)**.** The town of Königsberg (now called Kaliningrad) was built on an island in the Pregel River. The island sat near where two branches of the river join, and the borders of the town spread over to the banks of the river as well as a nearby promontory. Between these four land masses, seven bridges had been erected. The townsfolk used to amuse themselves by crossing over the bridges and asked whether it was possible to find a trail starting and ending in the same location allowing one to traverse each of the bridges exactly once. Figure 7.4 has a graph-theoretic model of the town, with the seven edges of the graph representing the seven bridges. By Theorem 7.69, this graph is not Eulerian so it is impossible to find a trail as the townsfolk asked.

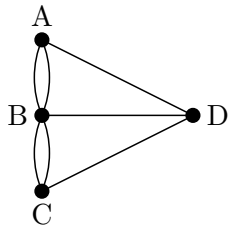


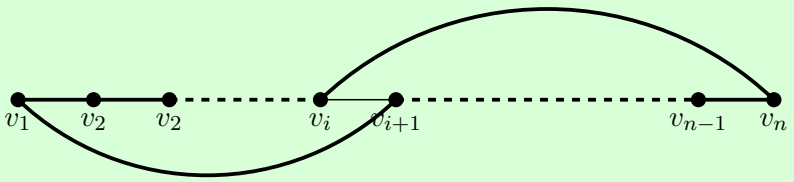
Figure 7.4: Model of the bridges in Königsberg from Example 7.70.

Definition 7.71. *A* **Hamiltonian cycle** *in a graph is a cycle passing through every vertex. G is* **Hamiltonian** *if it contains a Hamiltonian cycle.*

Unlike Theorem 7.69, there is no simple characterization of all graphs with a Hamiltonian cycle. In fact, the problem of determining whether or not a graph contains a Hamiltonian cycle is one of the most famous *NP-Complete* problems. The details are beyond the scope of this book, but briefly (and oversimplifying a bit), *NP-Complete* is a class of problems that are all equivalent in the sense that if any of them can be solved in polynomial time, then they can all be solved in polynomial time. Further, nobody currently knows whether or not any of them can be solved in polynomial time. This leads to the so-called *P versus NP* problem, one of the most important open problems in theoretical computer science. (Again, the details of precisely what this means are beyond the scope of this book.)

Coming back to the Hamiltonian cycle problem, we do have the following one-way result.

Theorem 7.72 (Dirac's Theorem, 1952)**.** *Let $G = (V, E)$ be a graph with $n = |V| \geq 3$ vertices where each vertex has degree $\geq \frac{n}{2}$. Then G is Hamiltonian.*

> **Proof:** *Arguing by contradiction, suppose G is a maximal non-Hamiltonian graph with $n \geq 3$, and that G has more than 3 vertices. Then G cannot be complete. Let a and b be two non-adjacent vertices of G. By definition of G, $G+ab$ is Hamiltonian, and each of its Hamiltonian cycles must contain the edge ab. Hence, there is a Hamiltonian path $v_1v_2 \dots v_n$ in G beginning at $v_1 = a$ and ending at $v_n = b$. Put*
>
> $$S = \{v_i : av_{i+1} \in E\} \qquad \text{and} \qquad \{v_j : v_jb \in E\}.$$
>
> *As $v_n \in S \cap T$, we must have $|S \cup T| = n$. Moreover, $S \cap T = \varnothing$, since if $v_i\S \cap T$ then G would have the Hamiltonian cycle*
>
> $$v_1v_2 \cdots v_iv_nv_{n-1} \cdots v_{i+1}v_1,$$
>
> *as in the following figure, contrary to the assumption that G is non-Hamiltonian.*
>
> 
>
>
> *But then*
>
> $$d(a) + d(b) = |S| + |T| = |S \cup T| + |S \cap T| < n.$$

But since we are assuming that $d(a) \geq \frac{n}{2}$ *and* $d(b) \geq \frac{n}{2}$*, we have arrived at a contradiction.* □

7.6.3 Planar Graphs

Definition 7.73. *A graph is* **planar** *if it can be drawn in a plane with no intersecting edges. Such a drawing is called a* **planar embedding** *of the graph.*

Example 7.74. Although the usual way K_4 is drawn has two edges intersect, it is planar as shown in figure 7.5. It is important to understand that being planar means you *can* draw it with no intersecting edges, not that every way of drawing it has no edges intersecting.

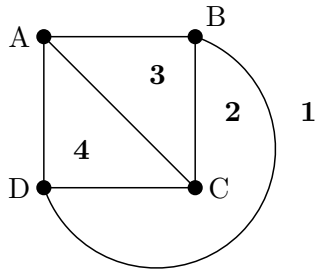


Figure 7.5: A planar embedding of K_4.

★**Exercise 7.75.** Draw a planar embedding of K_4 that does not have curved edges.

Definition 7.76. *A* **face** *of a planar graph is a region bounded by the edges of the graph.*

Example 7.77. K_4 has 4 faces, labeled 1 through 4 in Figure 7.5. Face **1**, which extends indefinitely, is called the *outside face.*

Here are a few results about planar graphs. These theorems use v and e instead of n and m because although computer scientists often use n and m, graph theorists seem to prefer v and e. And you should get used to the fact that not everybody uses the same notation, so it's good for you to see different letters used.

Theorem 7.78 (Euler's Formula)**.** *For every drawing of a connected planar graph with* v *vertices,* e *edges, and* f *faces the following formula holds:*

$$v - e + f = 2.$$

Proof: *The proof is by induction on e. Let $P(e)$ be the proposition that $v-e+f = 2$ for every drawing of a graph G with e edges. If $e = 0$ and it is connected, then we must have $v = 1$ and hence $f = 1$, since there is only the outside face. Therefore, $v - e + f = 1 - 0 + 1 = 2$, establishing $P(0)$*

Assume now $P(e)$ is true, and consider a connected graph G with $e+1$ edges. Either

❶ *G has no cycles. Then there is only the outside face, and so $f = 1$. Since there are $e + 1$ edges and G is connected, we must have $v = e + 2$. This gives $(e + 2) - (e + 1) + 1 = 2 - 1 + 1 = 2$, establishing $P(e + 1)$.*

❷ *or G has at least one cycle. Consider a spanning tree of G and an edge uv in the cycle, but not in the tree. Such an edge is guaranteed by the fact that a tree has no cycles. Deleting uv merges the two faces on either side of the edge and leaves a graph G' with only e edges, v vertices, and f faces. G' is connected since there is a path between every pair of vertices within the spanning tree. So $v - e + f = 2$ by the induction assumption $P(e)$. But then*

$$v - e + f = 2 \implies (v) - (e + 1) + (f + 1) = 2 \implies v - e + f = 2,$$

establishing $P(e + 1)$.

This finishes the proof. □

Theorem 7.79. *(a) Every simple planar graph with $v \geq 3$ vertices has $e \leq 3v - 6$ edges.*

(b) Every simple planar graph with $v \geq 3$ vertices and which does not have C_3 as a subgraph has $e \leq 2v - 4$ edges.

Proof: *If $v = 3$, both statements are plainly true so assume that G is a maximal planar graph with $v \geq 4$. We may also assume that G is connected, otherwise, we may add an edge to G. Since G is simple, every face has at least 3 edges in its boundary. If there are f faces, let F_k denote the number of edges on the k-th face, for $1 \leq k \leq f$. We then have*

$$F_1 + F_2 \cdots + F_f \geq 3f.$$

Also, every edge lies in the boundary of at most two faces. Hence if E_j denotes the number of faces that the j-th edge has, then

$$2e \geq E_1 + E_2 + \cdots + E_e.$$

Since $E_1 + E_2 + \cdots + E_e = F_1 + F_2 \cdots + F_f$, we deduce that $2e \geq 3f$. By Euler's Formula we then have $e \leq 3v - 6$.

The second statement follows for $v = 4$ by inspecting all graphs G with $v = 4$. Assume then that $v \geq 5$ and that G has no cycle of length 3. Then each face has at least four edges on its boundary. This gives $2e \geq 4f$ and by Euler's Formula, $e \leq 2v - 4$. □

To be clear, Theorem 7.79 part (a) implies that a graph with at least 3 vertices and more than $3v - 6$ edges cannot be planar (the contrapositive of the statement). Similarly for part (b).

Example 7.80. K_5 is not planar by Theorem 7.79 since K_5 has $\binom{5}{2} = 10$ edges and $10 > 9 = 3(5) - 6$.

★**Exercise 7.81.** Prove that $K_{3,3}$ is not planar.

Answer

7.6.4 Minimum Spanning Trees

Recall that a **spanning tree** of G is a subgraph T of G which is a tree that spans G. In other words, it contains all of the vertices of G. Some problems can be boiled down to trying to find a spanning tree of a weighted graph such that the sum of the weights of all of the edges of the spanning tree is as small as possible. This section formally defines this problem and then presents two algorithms to solve it.

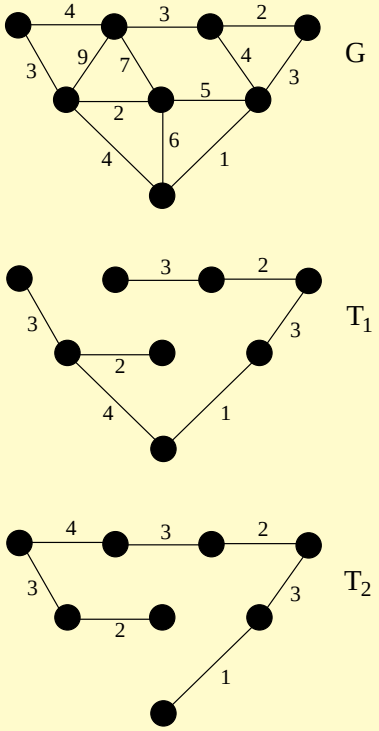
Definition 7.82. *If T is a tree, the* **weight** *of a T is the sum of the weights of its edges. That is,*

$$w(T) = \sum_{(u,v)\in T} w(u,v).$$

Definition 7.83. *Let $G = (V, E)$ be a connected, weighted graph. A* **minimum spanning tree (MST)** *of G is spanning tree T of minimum weight.*

It should be clear that a minimum spanning tree always exists.

Example 7.84. Here is an example of a graph G along with two different minimum spanning trees of G, T_1 and T_2. Notice that $w(T_1) = w(T_2) = 18$, and try as you might, you will be unable to find a spanning tree of weight less than 18.

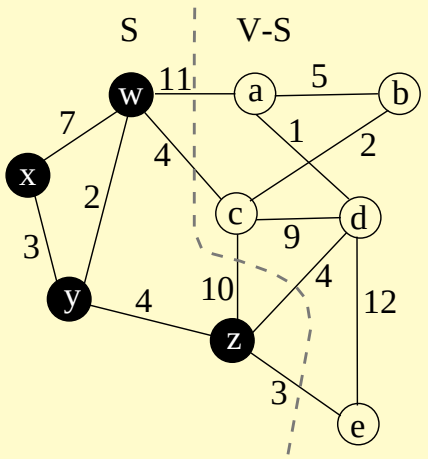


Minimum spanning trees can be constructed in a greedy fashion. There are two common algorithms to construct MSTs, **Kruskal's algorithm** and **Prim's algorithm**. Both of these algorithms use the same basic ideas, but in a slightly different fashion. In the rest of this section we will consider a general approach to find MSTs, prove that the general approach works, and show how to implement Kruskal's and Prim's algorithms based on the approach.

Definition 7.85. *Let $G = (V, E)$ be a connected, weighted graph.*

- *A* **cut** *$(S, V - S)$ of G is a partition of the vertices V.*
- *An edge $(u, v) \in E$ is said to* **cross** *the cut if one of the endpoints is in S, and the other is in $V - S$.*
- *The set of edges which cross a cut are the* **cross edges**.
- *A cut* **respects** *a set A of edges if A does not contain any cross edges.*
- *A cross edge of minimum weight is called a* **light edge**.

Example 7.86. Here is an example of some of the terminology applied to graph.



S={x,y,z,w}

V-S={a,b,c,d,e}

(w,a) and (c,z) are cross edges

(z,e) is a light edge

The cut respects {(x,w),(y,w),(c,d)}

The cut does not respect {(a,b),(d,z)}

The generic MST algorithm can be described as follows. Let A be the edges a minimal spanning tree of G. The MST algorithm "grows" the spanning tree one edge at a time. It starts with set $A = \emptyset$, which is clearly a subset of every minimum spanning tree. At each step, the algorithm adds an edge (u, v) to A so that the set $A \cup \{(u, v)\}$ is a subset of some minimum spanning tree. Such an edge (u, v) is called a **safe edge**, because we can safely add it to the set A and still continue.

The algorithm is simple:

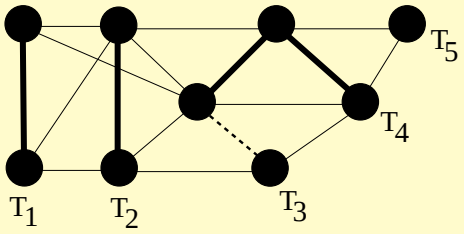
Procedure 7.87. *The generic MST algorithm.*

```
MST(G)
 A=EmptyList
 While NOT IsSpanningTree(G,A)
      e = SafeEdge(G,A)
      Insert(A,e)
 return A
```

In some sense, this is not technically an algorithm. Why? In order for it to be an algorithm, we need each step to be clearly executable. But there are at least two steps that are unclear. First, how does `IsSpanningTree(G,A)` determine whether or not A is a spanning tree of G? Second, how does `SafeEdge(G,A)` find a safe edge? Until we answer these questions we really just have a vague outline of an algorithm.

We will start by attempting to address the first question. Consider A, the partial set of edges that we are building into a spanning tree during the MST algorithm Notice that the graph $G_A = (V, A)$ is a forest, with some of the trees consisting of just a single node, and that each tree in the forest G_A is a **connected component**. At every step of the algorithm, MST adds an edge to the set A. which results in the merger of two trees into one.

Example 7.88. Consider the graph below where the edges of A are darkened and we have labeled the trees of the forest T_1 through T_5. If we add the dashed edge to A in the next step, the result will be that trees T_3 and T_4 will be merged into a single tree.



So what does this have to do with determining whether or not A is a spanning tree? Simple: At the beginning, $|A| = 0$, and we have $|V|$ trees in the forest, one for each vertex. At each step of the algorithm, we merge two trees. Therefore, all we have to do is iterate through $|V| - 1$ times and we will be left with a single tree–a spanning tree!

Now the harder question: how do we find safe edges. But first, a question that may have occurred to you: How do we know that there are any safe edges? The algorithm assumes they exist, so we need to be certain that they always do. Luckily, we defined safe edges in such a way that that *have to* exist as long as we follow the algorithm correctly. Let us argue this so it is more clear.

At the beginning of the algorithm, $A = \emptyset$, and any edge in any minimum spanning tree is safe. Since we know at least one spanning tree exists, then any edge in that tree is safe. So we know we that at the beginning there are safe edges.

During each iteration, we add a safe edge to A. Recall that by definition a safe edge is an edge (u, v) such that the set $A \cup \{(u, v)\}$ is a subset of some minimum spanning tree. Thus, every time we add a safe edge, the revised set A is guaranteed to still be a subset of some minimum spanning tree T. Thus, any edge from $T - A$ is a safe edge, and since the algorithm has not finished yet, there must be at least one safe edge (i.e. some edge in T that is not in A. If that sounds a bit convoluted, it is not surprising. Read it slowly and carefully a few more times and I think you will eventually catch on.

Now we know there are safe edge, how do we find them?

Actually, it's not that hard to find safe edges, as we will see next.

We begin with an important result.

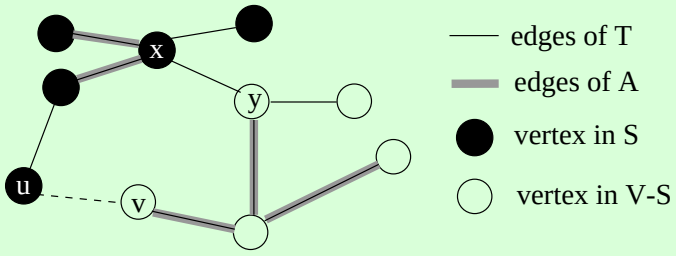
Theorem 7.89. *Let $G=(V, E)$ be a connected, weighted graph, and*

- *$A \subseteq E$ a subset of some MST for G,*
- *$(S, V - S)$ be any cut of G that respects A, and*
- *(u, v) be a light edge of $(S, V - S)$.*

Then the edge (u, v) is safe for A.

Proof: *The idea of the proof is as follows: Let T be a MST of G containing A, and (u,v) an edge as described above. If $(u,v) \in T$, then (u,v) is safe for A, and we are done. If $(u,v) \notin T$, we need to find an MST T' such that $A \cup \{(u,v)\} \subseteq T'$ (so that (u,v) is safe). In order to do this, we will find an edge $(x,y) \in T$ such that the tree $T' = (T - \{(x,y)\}) \cup \{(u,v)\}$ is an MST for G that contains A and (u,v). that will mean that (u,v) is safe for A.*

The only step of the proof that is not clear is how to find an edge $(x,y) \in T$ that will do as we desire. To see how we can do that, consider the following diagram of the situation.



Notice that the graph $T \cup \{(u,v)\}$ contains a cycle (since adding any edge to a tree will create a cycle). Since (u,v) is a cross edge on the cycle, there must be another cross edge on the cycle. Let (x,y) be such an edge. We claim that $T' = (T - \{(x,y)\}) \cup \{(u,v)\}$ is an MST for G containing A, so that (u,v) is safe for A. The edge (x,y) is not in A, because the cut respects A. Thus, A is a subset of T'. Now all we need to show is that T' is an MST for G.

Proof that T' is an MST of G: Since (x,y) is a cross edge and (u,v) is a light edge, $w(u,v) \leq w(x,y)$, which implies $w(u,v) - w(x,y) \leq 0$. Therefore,

$$w(T') = w(T) + w(u,v) - w(x,y) \leq w(T).$$

Since T is an MST, $w(T) \leq w(T')$. Thus, $w(T) = w(T')$, and T' is an MST for G.

To summarize, we have found a tree T' such that T' is an MST of G, A is a subset of T', $(u,v) \in T'$, and $(u,v) \notin A$, so (u,v) is safe for A. □

We can use Theorem 7.89 to prove the following.

Theorem 7.90. *$G=(V,E)$ be a connected, weighted graph, and*

- *$A \subseteq E$ a subset of some MST for G,*
- *C be the edges in a connected component of $G_A=(V,A)$, and*
- *(u,v) be a light edge of the cut $(C, V-C)$.*

Then (u,v) is safe for A.

Proof: *Since the cut $(C, V-C)$ respects A, this follows from Theorem 7.89.* □

★**Question 7.91.** In the previous theorem, why does the cut $(C, V - C)$ respects A?

Theorem 7.90 basically says that if C is a subtree of an MST, and (u, v) is an edge of minimum weight with exactly one endpoint incident with C, then $C \cup \{(u, v)\}$ is a subtree of an MST for G. Here are two ideas based on this theorem:

- **Idea 1:** Let u be a vertex of G, and (u, v) an edge of minimum weight incident with u. Then (u, v) is contained in some MST of G. (Here, $C = \{u\}$.)
- **Idea 2:** If (u, v) is an edge of minimal weight in G, then (u, v) is contained in some MST of G. (Again, $C = \{u\}$.)

Next we provide high level descriptions of Prim's and Kruskal's algorithm so you can hopefully see how they are each applying the ideas above. Then we will give more detailed descriptions of both.

Prim's algorithm uses Theorem 7.90 to build a single tree into an MST by starting at some vertex and "growing out" from it.

Example 7.92. Here is the idea of Prim's algorithm:

- Pick some vertex x.
- Let $A = \{(x, y)\}$, where edge (x, y) has minimum weight of edges incident with x.
- While A is not an MST
  - Add to A a minimum weight edge which has exactly one endpoint incident with A

On the other hand, Kruskal's algorithm sorts the edges of the graph according to weight, and adds edges (starting with the lightest) as long as they do not create a cycle until a spanning tree is created.

Example 7.93. The idea of Kruskal's Algorithm:

- Let $A = \emptyset$.
- While A is not an MST
  - Add to A a minimum weight edge that does not form a cycle.

★**Question 7.94.** Is Prim's Algorithm based on Idea 1 or 2? What about Kruskal's algorithm?

Next, we dig into details for both of these algorithms. Let us continue with Kruskal's algorithm. Here is a slightly more detailed description of Kruskal's algorithm that is adding a few important details that were missing.

Example 7.95. Kruskal's algorithm is as follows. Given a graph $G = (V, E)$, treat E as an array of edges.

- Sort E in ascending order.
- Set $A = \emptyset$
- For I = 1 to $|E|$
  If $A \cup \{E[I]\}$ does not contain a cycle
  $A = A \cup \{E[I]\}$
- Return A.

We still need to answer an important questions in order to have a complete algorithm: When does $A \cup \{E[I]\}$ contains a cycle? Notice that as the algorithm progresses, A is a forest. Edges connecting two vertices in the same tree will create a cycle. Edges that go from one tree to another will not create a cycle. So we will store each tree in a separate set. Adding an edge connect two trees, so we merge the sets. Based on these observations, we can now give a more detailed description of Kruskal's algorithm.

Procedure 7.96. *Kruskal's Algorithm*

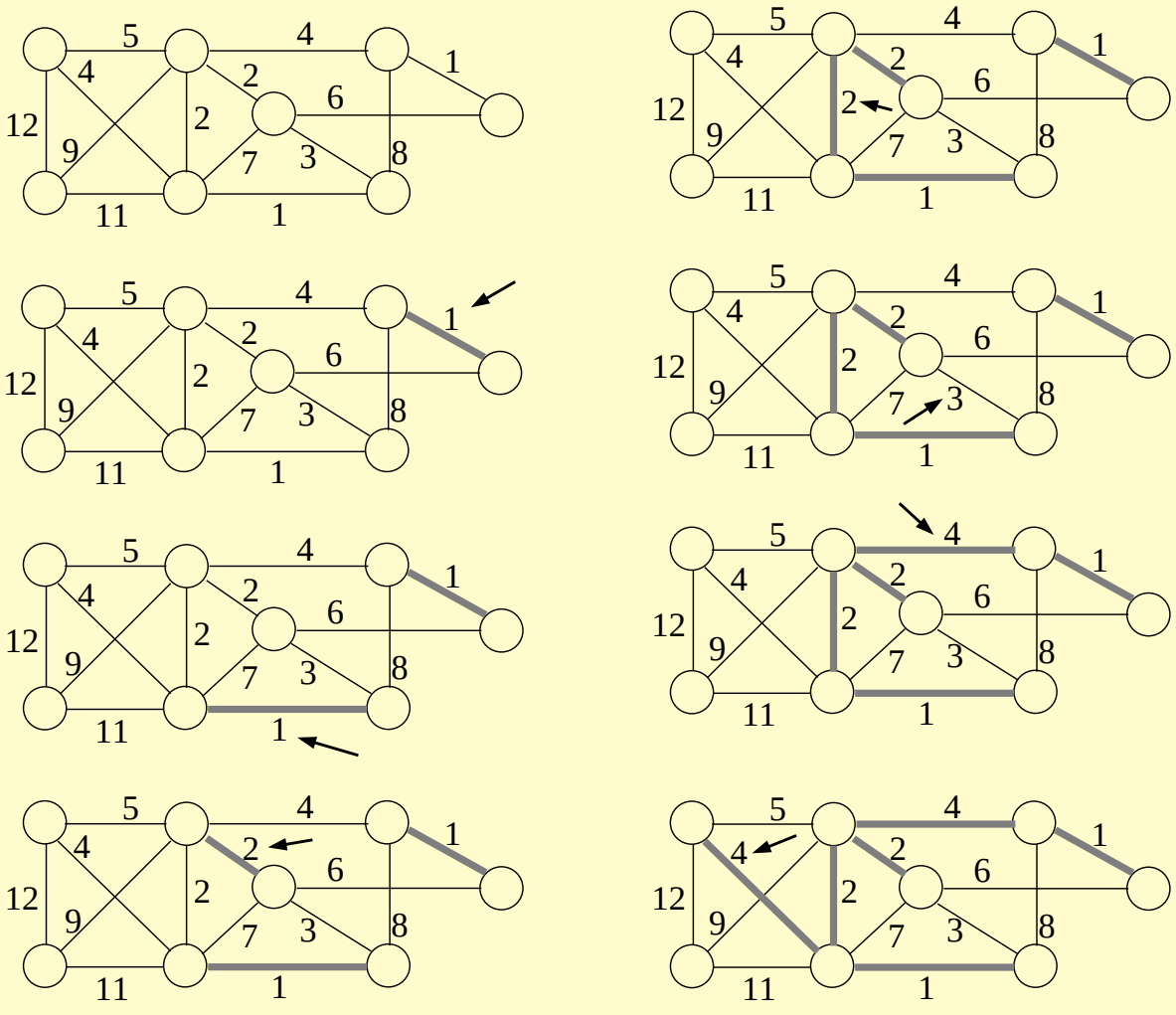
```
Kruskal_MST(G)
    A=EmptySet
    ForAll v in V[G]
        Create_Set(v)
    SortAscending(E[G])
    ForAll edges e=(u,v) in E[G] //in sorted order
        If Set(u) != Set(v)
            Insert(A,e)
            Set_Union(u,v)
    Return A
```

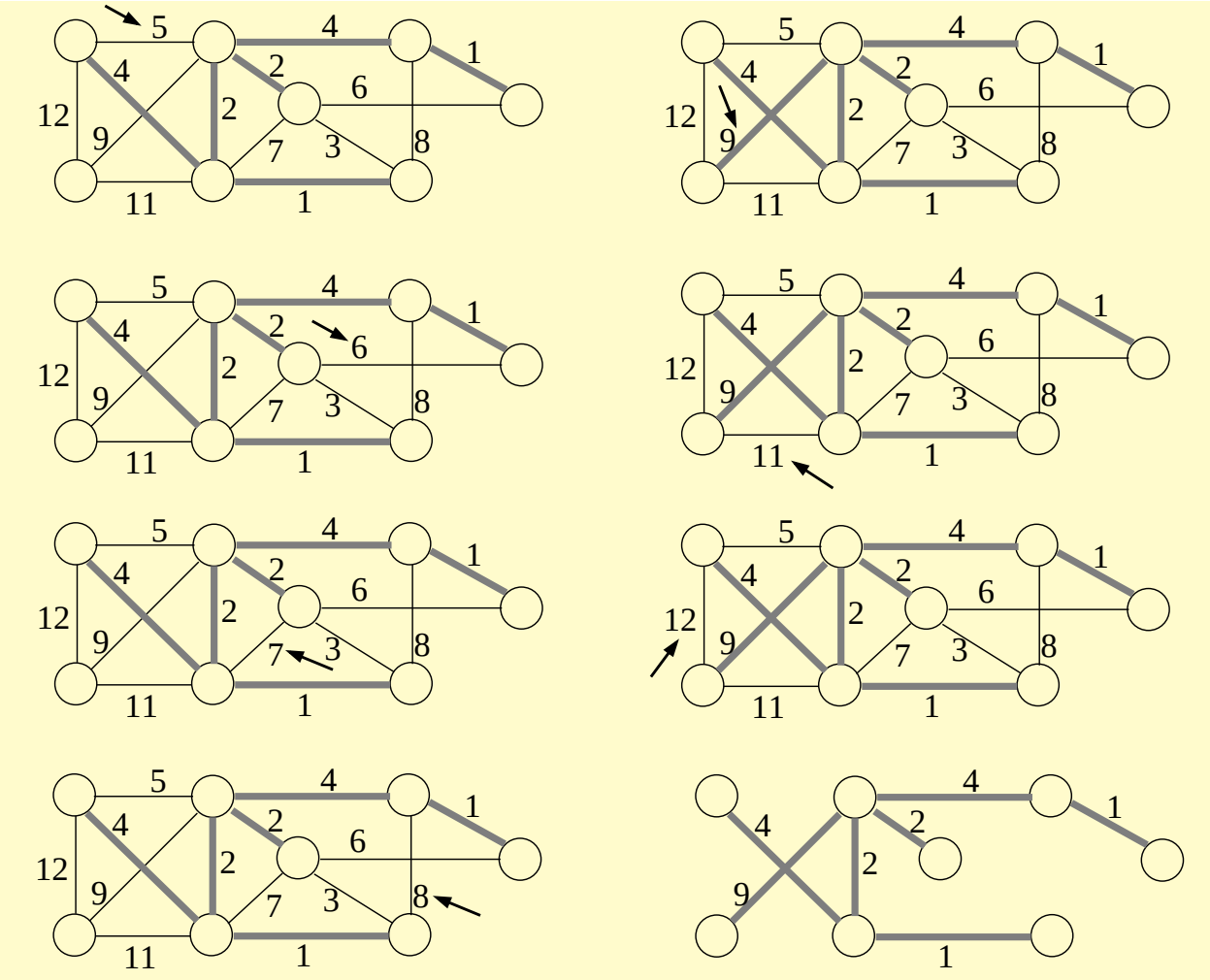
There are still important unanswered questions that we will not answer, but we will ask: How do we implement the set data structure we need? It needs to store sets in a way that allows it to determine if two elements are in the same set and create the union of two sets. One solution is to use something called **union-find algorithm** (or **union-find data structure**). Unfortunately, we do not have time to go into the details of this data structure.

Now that we have the algorithm, how good is it? Let $n = |V|$ and $m = |E|$. Creating the sets takes $O(n)$ time (constant time for each). Sorting the edges takes $O(m \log m)$ time. With a union-find data structure, it is possible to implement the sets so that comparing and unioning sets each take $O(\log n)$ time, and adding an edge to A takes constant time. Since these operations are done at most m times (one for each edge), the cost of the `ForAll` loop is $O(m \log n)$. Therefore, the complexity of Kruskal's Algorithm is $O(m \log m) + O(m \log n) = O(m \log m) = O(m \log n)$.

★**Question 7.97.** Why is $O(m \log m) = O(m \log n)$?

Example 7.98. Here is an example of Kruskal's algorithm (Follow down the columns here and then on the next page). Note that we are not showing the details about the sets in this example, but following along like you would if you did it by hand.





Before discussing Prim's algorithm, we first need a new data structure called a *priority queue*.

Definition 7.99. *A* **priority queue** Q *is a data structure that supports the following operations.*

- `Q.insert(Item v,Key k)` *inserts the Item* v *into* Q *using the value of the Key* k *to determine where it goes.*
- `Q.extractMin()` *removes and returns an Item from* Q *that has a minimum key value. If there are multiple items with the same minimum key value, which one gets returned depends on the implementation. Most algorithms that use priority queues do not care about which order tied keys are returned in.*
- `Q.decreaseKey(v,k)` *decreases the key value for Item* v *to* k *and moves it to the appropriate place in* Q *based on the new key value.*
- `Q.insertAll(Item[] values,Key[] keys)` *inserts the Items from the list values based on the corresponding keys into* Q*.*

There are multiple ways to implement a priority queue that has these operations. A common choice, the *min heap*, allows us to implement the priority queue so that the first three operations

take $O(\log n)$ time if Q contains n items, and the last one takes $O(n)$ time to insert a list of size n into an empty Q.

Unlike Kruskal's algorithm, with Prim's algorithm we grow a single tree A into a minimum spanning tree. An arbitrary vertex r is picked, and the tree is grown from that vertex. At each step a light edge of the cut $(A, v - A)$ is added to A. That is, we add an edge that connects a new vertex to A. Since it adds a node not already connected to A, it remains a tree since it is impossible to add a cycle if the new vertex is not already connected to some vertex in A.

In order to implement the algorithm, we need to have an efficient (greedy) way to determine the light edge at each step. To help facilitate this, for each node x, we will store

- The $key(x)$ is the weight of the minimum weight edge that connects x to some vertex in A.
- The *predecessor* $p(x)$ is the vertex y in A such that $w(x, y) = key(x)$. That is, of all of the nodes in A, y is one such that $w(x, y)$ is as small as possible.

We choose some root vertex r to start growing our tree from and set $key(r) = 0$, and $p(r) = NULL$. Each node $x \neq r$ starts with $key(x) = \infty$ (or `MAX_INT` or whatever the largest value we can store is). As the algorithm progresses, the key and predecessor are continually updated to be the best possible. We do not need to initialize $p(x)$ since it will eventually get set for every node (except r) by the algorithm.

When the algorithm is finished, the minimum spanning tree can be constructed by using the values of p. For instance, if $p(a) = b$, then (b, a) is an edge of the tree.

The value $key(x)$ only changes if some neighbor of x is added to A. When we add a node y to A, we need to update the key values of the nodes adjacent to y. Specifically, for each vertex x adjacent to y, if x is not already in A and $w(x, y) < key(x)$, then we have found a cheaper way to connect x to A, so we update the key and predecessor of x.

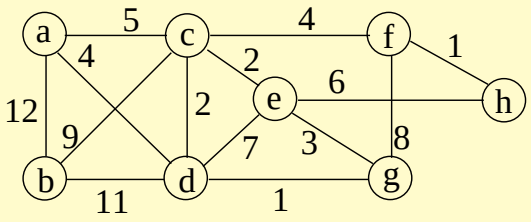
We will store the vertices in $V - A$ in a *priority queue* Q based on $key(x)$. This allows us to pick the minimum weight edge to add to A at each step.

We are now ready for the full version of the algorithm.

Procedure 7.100. *Prim's Algorithm*

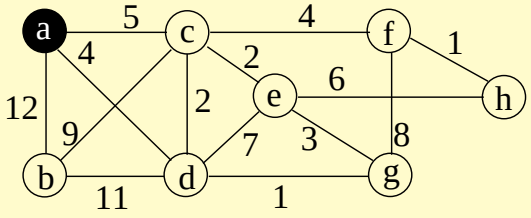
```
Prim_MST(G,r)
  PriorityQueue Q   // An empty priority queue
  Vertex[] p        // An array to store the predecessors
  int[] key         // An array to store the keys
  ForAll u in G(V)  // Start all keys out at the largest possible value
      key[u]=Max_Int
  key[r]=0     // r has the lowest key so it get extracted first
  p[r]=NULL    // r will never have a predecessor since it is the root
  Q.insertAll(V,key) // Add all vertices to Q based on key values
  While NotEmpty(Q)      // Extract vertices one at a time until
      u=Q.extractMin()  //    until we have a spanning tree
      ForAll v adjacent to u  // See if we need to update neighbors
        if(v in Q and w(u,v) < key[v]) // If we found a cheaper edge:
            key[v]=w(u,v)                // update the key value
            Q.decreaseKey(v,key[v])      // update the location of v in Q
            p[v]=u                       // update the predecessor
```

Example 7.101. Here is an example of Prim's algorithm starting from root $r = a$. Note: the diagram uses *nil* instead of *null* and k instead of *key* to save space. The values of k (key), p and, Q are shown at every step. The blackened nodes are in A and no longer in Q. Notice that the values of k for these nodes are also crossed out–that's just to make it more apparent visually which nodes are no longer in Q.



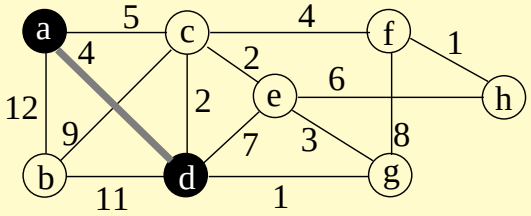
v	a	b	c	d	e	f	g	h
k	0	∞	∞	∞	∞	∞	∞	∞
p	nil	?	?	?	?	?	?	?

Q=[a,b,c,d,e,f,g,h]



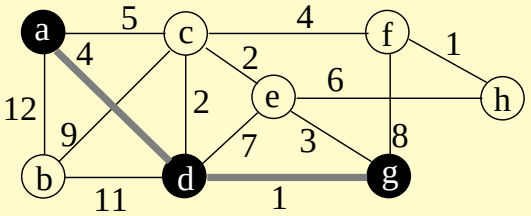
v	a	b	c	d	e	f	g	h
k	~~0~~	12	5	4	∞	∞	∞	∞
p	nil	a	a	a	?	?	?	?

Q=[d,c,b,e,f,g,h]



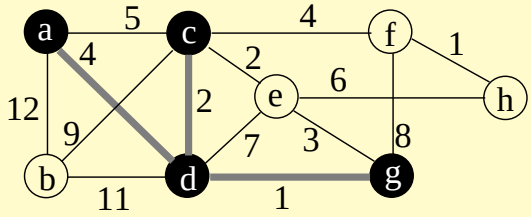
v	a	b	c	d	e	f	g	h
k	~~0~~	11	2	~~4~~	7	∞	1	∞
p	nil	d	d	a	d	?	d	?

Q=[g,c,e,b,f,h]



v	a	b	c	d	e	f	g	h
k	~~0~~	11	2	~~4~~	3	8	~~1~~	∞
p	nil	d	d	a	g	g	d	?

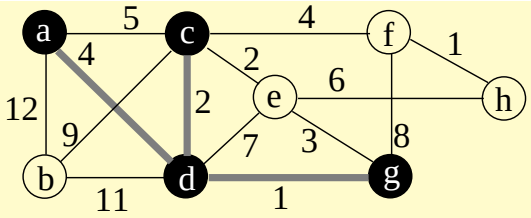
Q=[c,e,f,b,h]



v	a	b	c	d	e	f	g	h
k	~~0~~	9	~~2~~	~~4~~	2	4	~~1~~	∞
p	nil	c	d	a	c	c	d	?

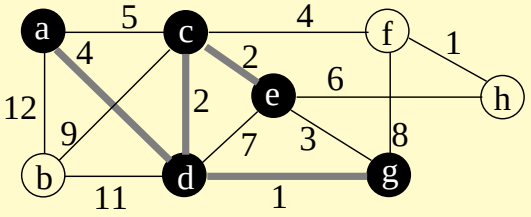
Q=[e,f,b,h]

The algorithm continues on the next page, but let's make a few observations before you continue. The gray lines show the MST edges, which can be found by looking at $p(x)$ for vertices x that are in A. For instance, on the third row notice that $k(d)$ is crossed out and $p(d) = a$. That means (a, d) is an edge in the tree. On the same line, $p(e) = d$, but that does not mean (d, e) is a tree edge because the algorithm has yet to confirm whether or not that is the cheapest way to connect to e. In fact, as you will see on the next page, it is not.



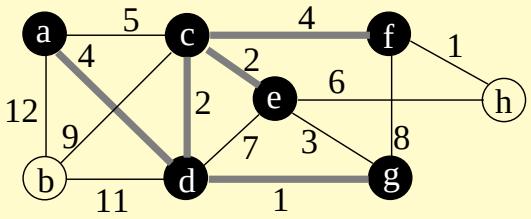
v	a	b	c	d	e	f	g	h
k	~~0~~	9	~~2~~	~~4~~	2	4	~~1~~	∞
p	nil	c	d	a	c	c	d	?

Q=[e,f,b,h]



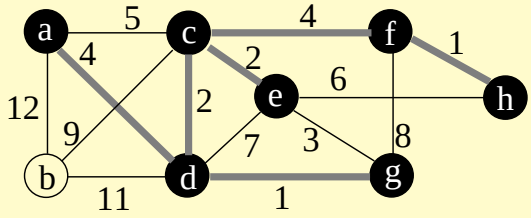
v	a	b	c	d	e	f	g	h
k	~~0~~	9	~~2~~	~~4~~	~~2~~	4	~~1~~	6
p	nil	c	d	a	c	c	d	e

Q=[f,h,b]



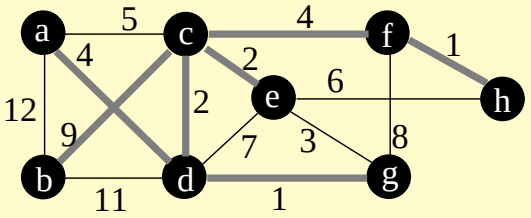
v	a	b	c	d	e	f	g	h
k	~~0~~	9	~~2~~	~~4~~	~~2~~	~~4~~	~~1~~	1
p	nil	c	d	a	c	c	d	f

Q=[h,b]



v	a	b	c	d	e	f	g	h
k	~~0~~	9	~~2~~	~~4~~	~~2~~	~~4~~	~~1~~	~~1~~
p	nil	c	d	a	c	c	d	f

Q=[b]



v	a	b	c	d	e	f	g	h
k	~~0~~	~~9~~	~~2~~	~~4~~	~~2~~	~~4~~	~~1~~	~~1~~
p	nil	c	d	a	c	c	d	f

Q=[]

★**Exercise 7.102.** Determine the computational complexity of `Prim_MST` given a graph with n vertices and m edges.

Time for a bonus algorithm to solve a new problem called the *single-source shortest path* problem. Here we are given a weighted graph $G = (V, E)$ and a chosen vertex r, and we wish to know the shortest path from r to every other node in the graph. We will not go into detail about this problem, but will simply present an algorithm to solve it that will look very familiar.

Procedure 7.103. *Dijkstra's Algorithm*

Dijkstra's Algorithm is almost identical to Prim's algorithm–the only differences are marked below with `<--`.

```
Dijkstra(G,r)
  PriorityQueue Q
  Vertex[] p
  int[] key
  ForAll u in G(V)
      key[u]=Max_Int
  key[r]=0
  p[r]=NULL
  Q.insertAll(V,key)
  While NotEmpty(Q)
      u=Q.extractMin()
      ForAll v adjacent to u
        if(v in Q and key[u]+w(u,v) < key[v]) <-- changed
            key[v]=key[u]+w(u,v)              <-- changed
            Q.decreaseKey(v,key[v])
            p[v]=u
```

Part of learning about algorithms is learning how we can apply what we have learned to solve various problems to solve other related, and sometimes not-so-related, problems. In this case, the minimum spanning tree and single source shortest path are definitely not the same problem, but they both are attempting to find spanning trees in the graph with certain properties. When you realize that, it makes sense that we might be able to slightly modify an algorithm for one problem to solve the other.

7.7 Reading Comprehension Questions

From Section 7.1

★**Question 7.1.** Draw an example of each of the following:

(a) An weighted undirected pseudograph

(b) An unweighted directed multigraph

(c) A network

★**Question 7.2.** Give an example of a problem that might be modeled using the following types of graphs. Make sure it is clear what the vertices and edges represent.

(a) A network

(b) An directed weighted multigraph.

(c) An unweighted undirected pseudograph

★**Question 7.3.** Prove that a graph with n vertices has at most $\binom{n}{2}$ edges. (There are several possible ways to prove this. You can use counting techniques or induction, for instance.)

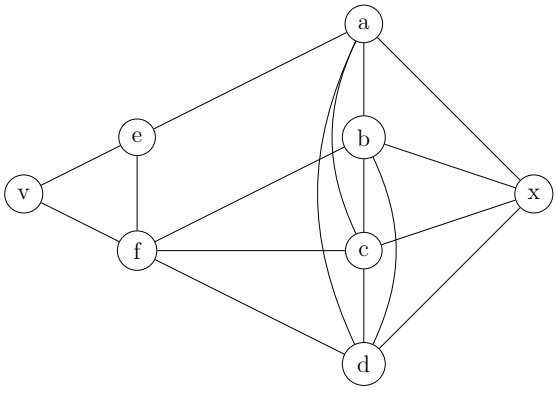
From Section 7.2

★**Question 7.4.** Draw an unconnected graph such that one component contains a cycle of length 4 and another component is a tree.

★**Question 7.5.** (a) How many edges does a tree with $n \geq 2$ vertices have? Draw a few trees of various sizes and you should see an obvious pattern.

(b) (a bit challenging) Prove that your formula is correct. (Hint: Use induction. But you have to be a little careful in how you do it. Also, you may assume that every tree contains at least one vertex with degree 1.)

★**Question 7.6.** answer the following questions about graph L below.



(a) Is L weighted or unweighted?

(b) Is L directed or undirected?

(c) Are e and x adjacent? Are f and b adjacent?

(d) Is L connected?

(e) How many vertices does L have?

(f) How many edges does L have?

(g) What is $\deg(v)$? $\deg(c)$?

(h) What is $\sum_{v \in L} \deg(v)$? Does this number seem to be related to your answer from (e)? Explain.

(i) Draw a spanning tree of L. How many edges does it have? Does your spanning tree contain any cycles? Explain why or why not.

(j) What is the minimum number of edges that you can remove to make the graph disconnected (that is, not connected)? Which ones?

(k) Find a cycle of length 3 in L. Then find one of length 4. Repeat for 5, 6, 7, and 8.

From Section 7.3

★**Question 7.7.** Draw K_6.

★**Question 7.8.** Draw C_8.

★**Question 7.9.** Draw P_5.

★**Question 7.10.** Draw Q_5. Just kidding. That would be a bit difficult to visualize. Instead, describe how you could construct Q_5 recursively. For instance, can you see how to go from Q_1 to Q_2? And from Q_2 to Q_3? And from Q_3 to Q_4? Once you observe the pattern it is pretty straightforward to see how to construct Q_{k+1} from Q_k.

★**Question 7.11.** Give a partition of the vertices of Q_3 to show that it is bipartite. In other words, which vertices go in V_1 and which go in V_2? Use 3-bit numbers to list the vertices (since that is the natural way to construct the graph).

★**Question 7.12.** Draw $K_{3,5}$. Then draw a graph G such that G is a subgraph of $K_{3,5}$.

From Section 7.4

★**Question 7.13.** Give an informal proof of Theorem 7.49. That is, argue why it makes sense by talking about edges, degrees, and vertices.

★**Question 7.14.** You are at a party with some friends and one of them claims "I just did a quick count, and it turns out that at this party, there are an odd number of people who have shaken hands with an odd number of other people at the party." Prove or disprove that this friend is correct.

From Section 7.5

★**Question 7.15.** (a) If a graph has very few edges, which representation is a better choice if space is the only consideration? Explain.

(b) If a graph has many edges, which representation is a better choice if space is the only consideration? Explain.

★**Question 7.16.** Are space considerations actually that important? In other words, practically speaking, if you can store a graph using one of the representation, can you store it in the other without worrying too much about space? Explain. (This is an important question, so think carefully about it!) (Hint: Think about storing the graph of friends on Facebook or another social media site.)

★**Question 7.17.** Given an *adjacency list* representation of a graph with n vertices and m edges, how long do the following operations take?

(a) Determine whether or not $(u, v) \in E$.

(b) Determine $\deg(u)$.

(c) Iterate over the neighbors of vertex u (assume u has k neighbors).

★**Question 7.18.** Given an *adjacency matrix* representation of a graph with n vertices and m edges, how long do the following operations take?

(a) Determine whether or not $(u, v) \in E$.

(b) Determine $\deg(u)$.

(c) Iterate over the neighbors of vertex u (assume u has k neighbors).

★**Question 7.19.** (a) If adding and removing *edges* is an important operation, is one of the representations a better choice? Explain.

(b) If adding and removing *vertices* is an important operation, is one of the representations a better choice? Explain.

From Section 7.6.2

★**Question 7.20.** (a) Is K_5 Eulerian? Explain.

(b) Is K_6 Eulerian? Explain.

(c) Is Q_3 Eulerian? If so, number the edges of Q_3 in order to demonstrate the Euler tour. If not, explain why not.

(d) Is Q_4 Eulerian? If so, number the edges of Q_3 in order to demonstrate the Euler tour. If not, explain why not.

(e) Is Q_3 Hamiltonian? If so, draw a Hamiltonian cycle on Q_3. If not, explain why not.

(f) Is Q_4 Hamiltonian? If so, draw a Hamiltonian cycle on Q_4. If not, explain why not.

(g) Is asking if C_7 is Hamiltonian a stupid question? Explain.

From Section 7.6.3

★**Question 7.21.** Give a planar embedding of $K_{2,3}$.

★**Question 7.22.** Does Theorem 7.79 imply that if a graph with $v \geq 3$ vertices has fewer than $3v - 6$ edges that it is planar? Explain, using an example if appropriate.

★**Question 7.23.** (a) Prove that Q_3 is planar.

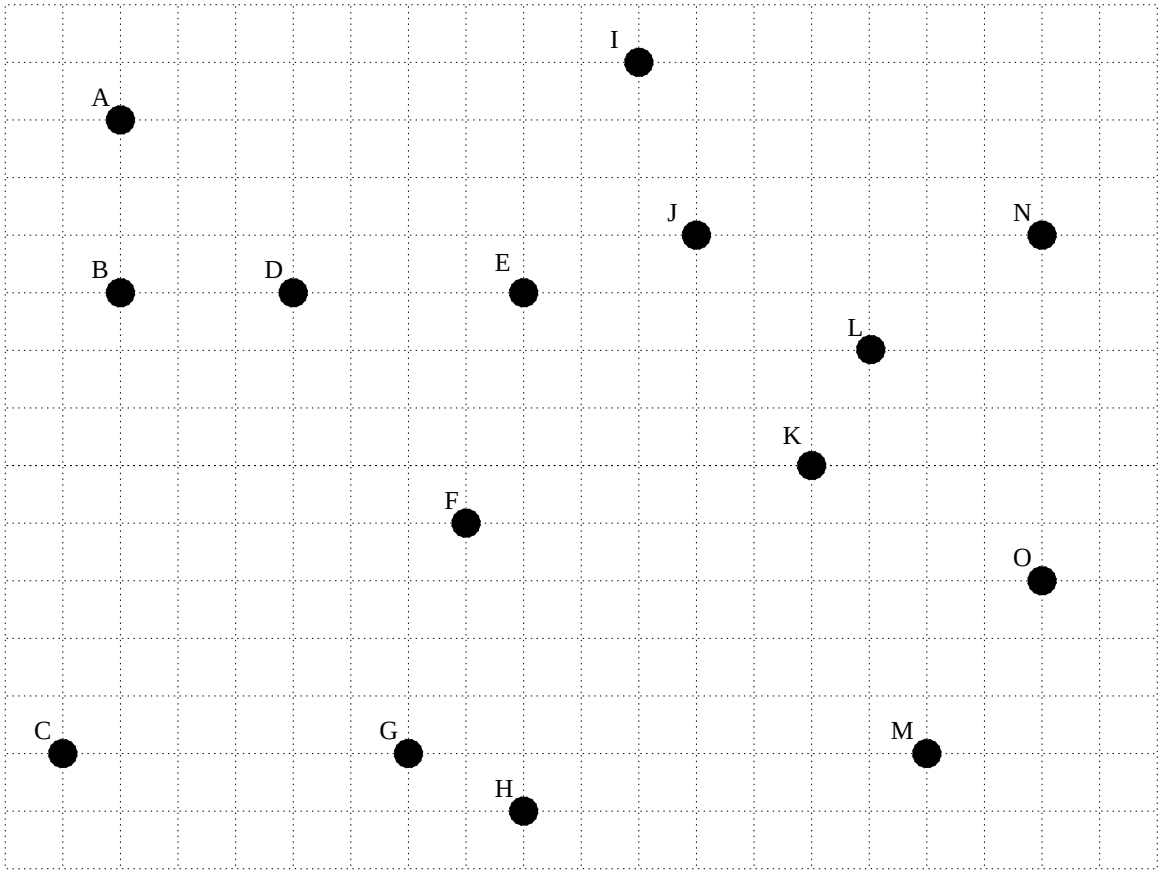
(b) Prove that Q_4 is not planar.

From Section 7.6.4

★**Question 7.24.** Can a graph have a minimum spanning tree with weight 34 and another with weight 35? Explain.

★**Question 7.25.** An Internet provider is installing an optical network in a rural town. They need to wire every house. The map below indicates the locations of the houses (dots). Each grid line represents 1 mile. They can route the cables anywhere they wish, and only need one connection to each house. Since optical cable is really expensive, the goal is to minimize the amount of cable required. An example: If they want to route from **I** to **J**, they could route south 3 miles, and east

1 mile for a total of 4 miles, but it would be better to route in a straight line from **I** to **J** for a cost of $\sqrt{3^2 + 1^2} = \sqrt{10} \approx 3.2$ miles.



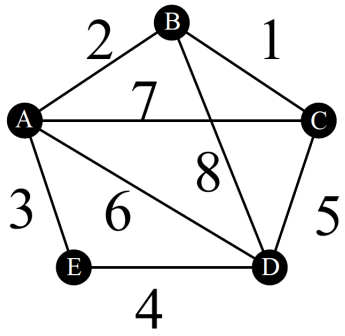
(a) Explain how this problem can be modeled as a graph problem. What are vertices? Edges? Is it directed? Weighted?

(b) Explain why solving this problem reduces to finding a minimum spanning tree of the graph.

(c) You will be asked to solve this problem in the next part. Should you use an algorithm like Prim's or like Kruskal's? Explain. (Note: I say an algorithm"like" because when humans run algorithms on graphs drawn on paper, they typically do not do them exactly as a computer would.)

(d) Compute a solution to this problem and give the total length of wire necessary.

★**Question 7.26.** Consider the following graph G with cut $S = \{A, B, C\}$ and $V - S = \{D, E\}$.



(a) List all of the cross edges.

(b) List all of the light edges.

(c) Which of the following edges crosses the cut: (A, B), (A, D), (D, E), (B, D).

(d) Find a minimum spanning tree of G and give its weight.

(e) Does G have more than one minimum spanning tree? Explain.

★**Question 7.27.** Can you think of a necessary condition for a graph to have more than one minimum spanning tree? Note: a *necessary condition* means a condition that has to be present for something to be true, but it being present does not always guarantee that it is true.

7.8 Problems

Problem 7.1. Give the degrees of the vertices of each of the following graphs. Assume m and n are positive integers. For instance, for P_n, $n-1$ of the vertices have degree 2, and 2 vertices have degree 1.

(a) C_n

(b) Q_n

(c) K_n

(d) $K_{m,n}$

Problem 7.2. Can a graph with 6 vertices have vertices with the following degrees: $3, 4, 1, 5, 4, 2$? If so, draw it. If not, prove it.

Problem 7.3. Prove or disprove that Q_n is bipartite for $n \geq 1$.

Problem 7.4. For what values of n is K_n bipartite?

Problem 7.5. Give the adjacency matrix representation of Q_3, numbering the vertices in the obvious order.

Problem 7.6. (a) Give the adjacency matrix representation for K_4.

(b) Give the adjacency list representation for K_4.

Problem 7.7. Describe what the adjacency matrix looks like for K_n for $n > 1$.

Problem 7.8. Describe what the adjacency matrix looks like for C_n for $n > 1$.

Problem 7.9. Given an adjacency matrix for C_n, with $n > 1$, how can you modify it to make it the adjacency matrix for P_n?

Problem 7.10. What property does the adjacency matrix of every undirected graph have that is not necessarily true of directed graphs?

Problem 7.11. Let G be a graph and let u and v be vertices of G.

(a) If G is *undirected* and there is a path from u to v, is there necessarily a path from v to u? Explain, giving an example if possible.

(b) If G is *directed* and there is a path from u to v, is there necessarily a path from v to u? Explain, giving an example if possible.

Problem 7.12. For what values of n is Q_n Eulerian? Prove your claim.

Problem 7.13. Is C_n Eulerian for all $n \geq 3$? Prove it or give a counter example.

Problem 7.14. Prove that K_n is Hamiltonian for all $n \geq 3$.

Problem 7.15. Prove that $K_{n,n}$ is Hamiltonian for all $n \geq 3$.

Problem 7.16. For what values of m and n is $K_{m,n}$ Eulerian?

Problem 7.17. A graph is Eulerian if and only if its adjacency matrix has what property?

Problem 7.18. What properties does an adjacency matrix for graph G need in order to use Theorem 7.72 to prove it is Hamiltonian?

Problem 7.19. Let G be a bipartite graph with v vertices and e edges. Prove that if $e > 2v - 4$, then G is not planar.

Problem 7.20. For each of the following, either give a planar embedding or prove the graph is not planar.

(a) Q_3

(b) Q_5

(c) $K_{2,3}$

(d) K_6

Problem 7.21. Let G be a graph with n vertices and m edges and let u and v be arbitrary vertices of G. Describe an algorithm that accomplishes each of the following assuming G is represented using an *adjacency matrix*. Then give a tight bound on the worst-case complexity of the algorithm. Your bounds might be based on n, m, $deg(u)$, and/or $deg(v)$.

(a) Determine the degree of u.

(b) Determine whether or not edge (u, v) is in the graph.

(c) Iterate over the neighbors of u (and doing something for each neighbor, but don't worry about what and assume it takes constant time for each neighbor).

(d) Add an edge between u and v.

Problem 7.22. Repeat Problem 7.21, but this time assume that G is represented using *adjacency lists*.

(a) Determine the degree of u.

(b) Determine whether or not edge (u, v) is in the graph.

(c) Iterate over the neighbors of u (and doing something for each neighbor, but don't worry about what).

(d) Add an edge between u and v.

Problem 7.23. (a) List several advantages that the adjacency matrix representation has over the adjacency list representation.

(b) List several advantages that the adjacency list representation has over the adjacency matrix representation.

Reading Question Solutions

1.1 A proposition is a statement that is either true or false.
1.2 The operators are *negation*, *or*, *and*, *exclusive-or*, *conditional*, and *biconditional*. See Table 1.1 and Table 1.2 for the truth tables.
1.3 $p \vee q$ is true if p is true, q is true, or both p and q are true, whereas $p \oplus q$ is true if and only if exactly one of p or q is true. So the difference is that is both p and q are true, $p \vee q$ is true, but $p \oplus a$ is false.
1.4 It is true unless p is true and q is false.
1.5 Here is a truth table with some intermediate columns to help. As long as you have the same final column, yours is probably fine.

p	q	$p \wedge q$	$\neg p$	$(p \wedge q) \vee \neg p$
T	T	T	F	T
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T

1.6 Here is a truth table with some intermediate columns to help. As long as you have the same final column, yours is probably fine.

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

1.7 By definition, no. If p is true, $\neg p$ is false, and if p is false, $\neg p$ is true.
1.8 q must be true since one of them has to be and p is not.
1.9 Nothing. It might be true, but it also might be false.
1.10 They are both true.
1.11 q has to also be false since $p \leftrightarrow q$ implies they have the same truth value.
1.12 In this case q also has to be true.
1.13 Since $p \rightarrow q$ is true whenever p is false, we cannot say anything about q, so it could be true or false.
1.14 By definition, if a proposition is a contingency, then it is *not* a tautology.
1.15 By definition, a proposition and its negation can *never* both be true. If the proposition is true, its negation is false, and if the proposition is false, its negation is true.
1.16 (a) $p \vee T$ is true if and only if either p or T is true. Since clearly T is true, $p \vee T$ is always true. Therefore, $p \vee T \ = T$. Alternatively, you can give a truth table for $p \vee T$ and then comment something like "since the final column of the truth table is always true, $p \vee T \ = T$." (b) We will do this one with a truth table: Notice that the column for $p \wedge F$ in the truth table below is always false. Therefore $p \wedge F = F$.

p	$p \wedge F$
T	F
F	F

1.17 You could draw a truth table and show that the columns for these two differ. However, there is any easier approach. Notice that if p is true and q is false, $\neg p \wedge \neg q$ is false, but $\neg(p \wedge q)$ is true. Therefore they are not equivalent.

1.18 We can't use the first reason because DeMorgan's law isn't the only rule we have to determine whether or not two propositions are equivalent. Perhaps they are equivalent by some other rule (in this case they aren't, which you should know if you answered the previous question). The second reason is also not valid because every proposition is equivalent to many other propositions that look different than it, so just knowing that they look different doesn't tell us anything. For instance, DeMorgan's law says that $\neg p \wedge \neg q = \neg(p \vee q)$. So even though those two don't look that same, they are equivalent.

1.19 Find an assignment of true values to the variables such that one is true and the other is false. That's all there is to it. Although sometimes this is easier said than done!

1.20 A propositional function is a statement that contains one or more variables and depending on the values of the variable(s), the statement is true or false. In other words, a propositional function is a function whose outputs are propositions.

1.21 $\neg\forall x P(x)$ means that it is not the case that $P(x)$ is true for all values of x. So it doesn't mean it is never true. It means that for one or more values of x it is false. That is, it means that it is not always true.

1.22 $\neg\exists x P(x)$ means that it is not the case that there is a value of x for which $P(x)$ is true. In other words, it is indeed saying that $P(x)$ is never true.

1.23 The two obvious alternatives are $\neg\exists x \exists y Q(x, y)$ and $\forall x \forall y \neg Q(x, y)$.

1.24 These are all equivalent: $\forall x \neg(x < 0 \wedge x > 0)$, $\forall x(\neg(x < 0) \vee \neg(x > 0))$, and $\forall x(x >= 0 \vee x <= 0)$.

1.25 $\forall x \exists y H(x, y)$.

1.26 Let $C(x, y)$ ="x changes at time y." Then $\neg C(x, y)$ ="x stays the same at time y." *If you did not define a predicate similar to this, stop reading now and try to come up with the rest of the answer using $C(x, y)$ before continuing to read.* Then the expression can be written as $\neg\exists x \exists y C(x, y) \wedge \neg\exists x \exists y \neg C(x, y)$, which of course can be simplified $\forall x \forall y \neg C(x, y) \wedge \forall x \forall y C(x, y)$ (but you would probably re-interpret this version in English as "Everything stays the same, everything changes," which if you think about is it essentially saying the same thing.).

1.27 (a) Given any integer, there is an integer that is at least as large as it. (b) There is an integer such that every integer is at least as large as it is. (c) They do not seem to be saying the same thing at all. (d) True. (e) False. (f) If the universe of discourse is changed to positive integers, then both statements are true. (The second one becomes true because every positive integer is at least as large as 1.) (g) No. Just because two statements have the same truth value, that does not mean they are saying the same thing. For instance, "1+1=2" is true and "$x^2 \geq 0$" is true, but they definitely are saying very different things.

1.28 $\neg p$, q, $\neg r$, r.

1.29 $\neg p$, $p \wedge r$, $\neg p \wedge r$, q, $\neg r$.

1.30 $\neg p$, $p \wedge r$, $q \vee \neg r$, $\neg p \wedge r$, $(p \wedge q) \vee (q \wedge \neg r) \vee \neg p$, $(p \wedge \neg r \wedge q) \vee (\neg p \wedge r \wedge \neg q) \vee (p \wedge r \wedge q) \vee (\neg p \wedge \neg r \wedge \neg q)$.

2.1 Answers will vary, but it should say something like "An argument using logic and/or math to demonstrate or show the nature of a conclusion," or "the process or an instance of establishing the validity of a statement especially by derivation from other statements in accordance with principles of reasoning" (the latter is from Merriam-Webster).

2.2 If someone correctly proves statement A, that means it is a true statement, regardless of whether or not you understand the proof. That's because, by definition, a proof establishes the validity of a statement.

2.3 True. An even integer is one of the form $2k$, where k is an integer. An odd integer is one of the form $2k+1$ where k is an integer. Thus, even numbers are divisible by 2 whereas odd numbers are not. A number cannot both be divisible by 2 and not divisible by 2 at the same time.
2.4 No. For instance, 6 is divisible by 2, but 2 is not divisible by 6.
2.5 No. A number cannot be both composite and prime because by definition, a composite integer is a positive integer $c > 1$ that is *not* prime. Thus, every integer greater than 1 is either prime or composite, but never both.
2.6 3, 97, 173, and 999983 are prime. 4, 6, 27, 38, 150, and 999985 are composite. 1 is neither. It is impossible to be both.
2.7 $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$. $7! = 7 \cdot 6! = 7 * 720 = 5040$, computed the easy way be recognizing I just needed to multiply the previous answer by 7.
2.8 Clearly $2! = 2$ is prime. We will show that this is the only case in which $n!$ is prime. $1! = 1$, which is not prime by definition. $3! = 2 \cdot 3$, which is clearly not prime. If $n > 3$, $n!$ is divisible by $3! = 3 \cdot 2$, so it not prime.
2.9 No. Take the example from the book, "If you know Java, then you know a programming language" (where A is the proposition "you know Java" and B is the proposition "you know a programming language." Since Java is a programming language, this proposition is true. Then B implies A is the proposition "if you know a programming language, then you know Java." But that is clearly not true. You might know *C++*, which is a programming language, but not know Java.
2.10 False. From the previous answer, consider the implication "if you know a programming language, then you know Java," and its inverse, "if you do not know a programming language, then you do not know Java." It shouldn't be too difficult to see that although the inverse is true, the implication is false.
2.11 This one is true since the inverse and converse of an implication are contrapositives of each other, and an implication and its contrapositive are equivalent.
2.12 An implication and its contrapositive are equivalent. Therefore, if one is true, then the other is true (and if one is false, the other is false, of course).
2.13 Your answer will likely be different, and hopefully more detailed than the one provided here. But you should say something about how you assume that what you want to prove is false, then use logic to arrive at a contradiction (that is, a statement that you know to be false). Since you "proved" a false statement using correct logic, it must be that your premise (that is, the statement that you assumed was false) is incorrect. Since your premise was that the statement you wanted to prove was false, then it must be that the statement is true (again, because you showed that if it is false, then you can prove something that is not true).
2.14 They are (cow, chicken, rabbit), (cow, rabbit, chicken), (chicken, cow, rabbit), (chicken, rabbit, cow), (rabbit, cow, chicken), and (rabbit, chicken, cow).
2.15 True. Every integer a can be written as $a = \frac{a}{1}$, where a and 1 are both integers and $1 \neq 0$, so it is rational.
2.16 Assume that k is the smallest positive rational number. Since k is rational, we can write it as p/q for integers p and $q \neq 0$. But clearly $k/2 = p/(2q)$ is positive, rational, and smaller than k, which contradicts our assumption that k was the smallest such number. Therefore there is no smallest positive rational number.
2.17 Since an implication and its contrapositive are equivalent, if you prove the contrapositive of a implication is true, then the implication must also be true. And that is exactly what proof by contraposition does.
2.18 **Contradiction:** Assume that p and $\neg q$ are both true. Get a contradiction. Conclude that if p is true, $\neg q$ cannot be true, so q must be true. Thus, $p \to q$ is true.
Contraposition: Prove that $\neg q \to \neg p$, which is equivalent to $p \to q$.

In both cases, you assume that $\neg q$ is true. Often the contradiction you get is that $\neg p$ is true (which is the goal in contraposition proof), so the majority of the proofs look the same. But they begin and end slightly differently.

2.19 True. From the Question 2.15, we know that every integer is rational, so integers are not irrational. Therefore, if a number is irrational, it cannot be an integer. Alternatively, you can recognize that this is essentially the contrapositive of the Question 2.15, so it is also true.

2.20 (a) Assume that $x > 0$ is irrational, but that $\sqrt{x}$ is rational. Then $\sqrt{x} = p/q$ for some integers $p, q \neq 0$. That means that $x = (\sqrt{x})^2 = (p/q)^2 = p^2/q^2$, which is clearly rational since p^2 and $q^2 \neq 0$ are both rational. But this contradicts our assumption that x is irrational. Therefore, $\sqrt{x}$ must be irrational.

(b) We will prove that if $\sqrt{x}$ is rational, then x is rational, which will imply our statement is true since this is the contrapositive of our statement. Assume $\sqrt{x}$ is rational. Then $\sqrt{x} = p/q$ for some integers $p, q \neq 0$. Therefore, $x = (\sqrt{x})^2 = (p/q)^2 = p^2/q^2$ which is clearly rational since p^2 and $q^2 \neq 0$ are both rational.

2.21 False. For instance, $1.5 = \frac{3}{2}$ is rational, but clearly not an integer.

2.22 We will use a proof by cases. Case 1: If n is even, then $n = 2k$ for some integer k. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is even since $2k^2$ is an integer. Case 2: If n is odd, then $n = 2k + 1$ for some integer k. Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd since $2k^2 + 2k$ is an integer. In both cases, the parity remains unchanged.

2.23 No you would have to show the reverse as well. That is, if I want to prove A if and only if B, I would have to prove either the proposition $(A \to B)$ or the contrapositive $(\neg B \to \neg A)$ **and** I would have to prove the inverse $(\neg A \to \neg B)$ or the converse $(B \to A)$.

2.24 (a) No. This is proving the forward direction twice by proving the implication and its contrapositive. One of these needs to be replaced with either the inverse or converse. (b) Yes. This is proving the contrapositive and the converse.

2.25 For the forward direction, we assume that n is even. Then $n = 2k$ for some integer k, so $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is even since $2k^2$ is an integer. Thus, n even implies n^2 is even. For the reverse direction, we will prove that n is not even implies n^2 is not even. In other words, n is odd implies that n^2 is odd. Assume n is odd. Then $n = 2k + 1$ for some integer k, so $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd since $2k^2 + 2k$ is an integer. Thus, n odd implies that n^2 is odd, which (as we have already said, but we'll say it again anyway) is equivalent to n^2 is even implies n is even.

2.26 You use proof by counterexample to *disprove* statements. You only need to show one instance where the statement is not true to demonstrate that it is not always true, so proof by counterexample is valid. On the other hand, proof by example is just demonstrating the truth of a statement given some specific values. Just because it works for the given values, that does not prove that it works for all values, so it is not a valid proof technique.

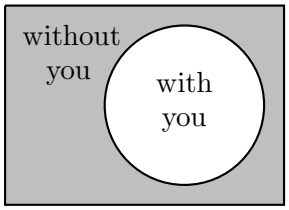
2.27 This is definitely *not* a valid proof technique! The problem is that when you write down an equation and start working both sides of it, you are implicitly assuming that the equation you are starting with is true. But since you are trying to prove that it is true, you can't start your proof with the fact that it is true–that is circular reasoning. For instance, do you remember the supposed proof of $-1 = 1$ that started by working both sides of the equation?

2.28 The step that divided both sides by $a - b$ was division by zero, which is not allowed!

3.1 (b), (d), (f) make sense. For the incorrect ones, first note that A and B are both sets of numbers. (a) does not make sense because an element cannot be a subset of a set. For (c), A contains the number 3, but not the set containing 3, which is what $\{3\}$ is. For (e), A does not contain as an element another set (i.e. B), so that notation does not make sense.

3.2 5. Remember, repeated elements do not count!

3.3 (a) i. Yes, ii. No, iii. No. (b) 6, 3, 4. (c) They are all finite sets.
3.4 (a) Yes (b) No (c) Yes (d) Yes (e) No
3.5 $\{n^3 | n \in \mathbb{Z}\}$
3.6 $\{n/100 | n \in \mathbb{Z}\}$
3.7 Yes (because the power set of A is the set of all subsets of A, and $A \subseteq A$, so $A \in P(A)$) and No (because the elements of $P(A)$ are subsets of elements of A, so a subset of $P(A)$ would be a set of subsets of A, but A is a set of elements (of whatever type A consists of). This is a subtle point, so do not worry too much about it unless you plan to major in mathematics.
3.8 $2^5 = 32$.
3.9 (a) $|A| = 5$ and $|P(a)| = 2^5 = 32$. (b) No. The elements of A are a, b, etc. If that statement were true, $\{a\} \in A$, but it is not. Remember, $a \in A$ (which is true) and $\{a\} \in A$ (which is not true) are not saying the same thing. (c) Yes. (d) No. As in part (b), the elements of A are a, b, etc. but $\{b, c, e\}$ is a set of those elements. Remember: $\in$ means "element of," and $\subseteq$ means "subset of," which are not the same thing! (e) Yes because each of the three sets in the set on the left are subsets of A. (f) No. To be a subset of the power set, it needs to be a set of subsets. This is a set of elements. (g) Yes because the set $\{b, c, e\} \subseteq A$.
3.10 (a) $\{a, b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z\}$ (b) $\{b, d, g, k, p, v\}$ (c) $\{a\}$ (NOT a!) (d) $\{a\}$ (e) $\{e, i, o, u\}$
3.11 (a) True; (b) False; (c) False; (d) True (This is DeMorgan's law in words)
3.12 (a) answers will vary, but should be things like $(1, z)$, $(3, x)$, and $(2, v)$. (b) answers will vary, but should be things like $(1, 2)$, $(3, 3)$, and $(4, 1)$. (c) 24. (d) $4^3 = 64$. (e) $2^{4^2 * 6} = 2^{96}$.
3.13 The area being pointed to is "with **AND** without you," so it is not at all correct. That is definitely not where Bono can't live. Notice that "with you" and "without you" are complements, so the Venn diagram to the right demonstrates a proper relationship between them. So where can't Bono live? He can't live anywhere in the rectangle (the universe) because he can't live in the circle ("with you") or outside the circle ("without you"). Put another way, the entire diagram is the place where Bono can't live.



Where Bono can't live

3.14 (a) $A \subseteq B$. (b) $A = B$.
3.15 First, $A \cap B$ is the set of elements that are in both A and B. Therefore, $\overline{A \cap B}$ is the set of elements that are not in both A and B. (This includes elements that are in A but not B, in B but not A, or in neither A nor B.) $\overline{A} \cup \overline{B}$ is the union of the elements that are not in A and the elements that are not in B. That is, it is any element that is either not in A or not in B. So it is all elements that are not in both A and B, which is exactly what $\overline{A \cap B}$ is. Therefore, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
3.16 First, notice that since U is the universal set, $A \subseteq U$ and $\overline{A} \subseteq U$. Let $x \in A \cup \overline{A}$. Then either $x \in A$ or $x \in \overline{A}$. In either case, $x \in U$ (since $A \subseteq U$ and $\overline{A} \subseteq U$). Therefore $A \cup \overline{A} \subseteq U$.

Now, assume $x \in U$. If $x \in A$, then $x \in A \cup \overline{A}$. If $x \notin A$, then by definition, $x \in \overline{A}$, and therefore $x \in A \cup \overline{A}$. In either case, $x \in A \cup \overline{A}$. Therefore $U \subseteq A \cup \overline{A}$.

Since we proved containment both ways, $A \cup \overline{A} = U$.
3.17 Given an integer a, compute a mod 2. If it is 0, a is even, and if it is 1, a is odd.
3.18 It certainly can be used. If the current time is t, and you are on 24-hour time, then in 8 hours the time will be $(t + 8$ mod 24. If you are using 12-hour time, it is a little more complicated. You can compute $(t + 8)$ mod 12 to get the time in 8 hours, but if the result is 0, you need to treat it like 12. Also, this does not take into account whether there was a switch from am to pm. That is more complicated and we would need to use additional logic to get that part correct.

3.19 Compute $c = a \bmod n$ and $d = b \bmod n$. According to Theorem 3.90, $c = d$ if and only if $a \equiv b \pmod{n}$. so just determine whether or not $c = d$.

3.20 $\gcd(524, 118) = 15$ as demonstrated here:

step	a	b	r
1	67890	12345	6165
2	12345	6165	15
3	6165	15	0
4	15	0	0

3.21 They are not because they have a common factor of 15.

3.22 No. In fact, they are usually not going to be the same (unless you start with an integer). As an example, the floor of 3.2 is 3, and the ceiling of 3 is 3, so the ceiling of the floor of 3.2 is 3. The ceiling of 3.2 is 4, and the floor of 4 is 4, so the floor of the ceiling of 3.2 is 4.

3.23 (a) $\mathbb{Z}$. (b) $\mathbb{Z}$. (c) $\{2z | z \in \mathbb{Z}\}$. That is, the set of all even numbers.

3.24 Here are possible answers. There are many other possible correct answers. (a) $f(x) = 2x$. (b) $f(x) = 6$. (c) $f(x) = 2x$. (d) $f(x) = 4$. (e) $f(x) = 2x$.

3.25 Here are possible answers. There are many other possible correct answers. (a) $f(x) = 2x$. (b) $f(x) = (2x) \bmod 6$ (so $f(4) = 2$ instead of 8). (c) Impossible. The domain only has 4 numbers, and the codomain has 6, so it is impossible to map to all of them. (d) $f(x) = 2x$ (it doesn't map to 10 or 12). (e) Impossible. Since an onto function is impossible, a bijective one is as well.

3.26 $(f \circ g)(x) = 2^{x+2}$ and $(g \circ f)(x) = 2^x + 2$. Did you get them backwards? If so, look at the definition of composition of functions again.

3.27 (a) False. If $a = b$, then clearly $f(a) = f(b)$, so that's meaningless. You need to show that if $f(a) = f(b)$, then $a = b$. (b) True. (c) False. That's the definition of a function. to show onto, you need to show that every element of the codomain gets mapped to by some element of the domain. (d) True. Since the range is the set of values actually mapped to, if it equals the codomain, then every value is mapped to and the function is onto. (e) False. For two reasons. First, elements of the range are always mapped to–that's the definition of range. Even if you change range to codomain, it is still false. You only need to show that there is at least one element of the codomain that is not mapped to. (f)True.

3.28 First, notice that if $f(a) = f(b)$, then $a^3 - 8 = b^3 - 8$, which implies $a^3 = b^3$. Taking the third root of each side, we get $a = b$. Thus, f is one-to-one. Now, notice that if $x \in \mathbb{R}$, then $\sqrt[3]{x+8} \in \mathbb{R}$, and $f\left(\sqrt[3]{x+8}\right) = \left(\sqrt[3]{x+8}\right)^3 - 8 = x + 8 - 8 = x$, so f is onto. To find the inverse (which I already did in order to prove it was onto, but I'll show the work anyway), we solve $y = x^3 - 8$ for x. We get $x^3 = y + 8$, so $x = \sqrt[3]{y+8}$. Replacing variables, we have that $f^{-1} = \sqrt[3]{x+8}$.

3.29 (a) $C = \{1, 3, 5, 7, 9\}$. (b) $C = \{1, 2, 3, 5, 7, 9\}$ (or any set that contains all of 1,3,5,7,9, and at least one of 2, 4, 6, 8, or 10). (c) $C = \{1, 3, 7, 9\}$ (or any proper subset of $\{1, 3, 5, 7, 9\}$). (d) $C = \{1, 3, 5\}$ and $D = \{7, 9\}$ (or any two disjoint sets such that $C \cup D = \{1, 3, 5, 7, 9\}$. (e) $C = \{1, 2, 3, 5\}$ and $D = \{7, 9\}$ (or many other possibilities).

3.30 Yes. It is a subset of $\mathbb{Z} \times \mathbb{Z}$.

3.31 There are many possible answers. Here is one. Define T to be the relation on human beings such that xTy if and only if x is at least as tall as y. It is not hard to see that T is reflexive, anti-symmetric, and transitive, so it is a partial order.

3.32 answers we vary, but here is one possibility. Let C be the set of all cars. Define the relation R on C by xRy if and only if x was manufactured in the same year as y. It is not hard to see that R is symmetric, reflexive, and transitive, so it is an equivalence relation. Let C_y be the set of all cars manufactured in year y. Then it is not hard to see that $C = C_{1886} \cup C_{1887} \cup \cdots \cup C_{2023} \cup C_{2024} \cup C_{2025}$ is a partition of C (assuming you aren't reading this in 2026 or later, and assuming we regard 1886

as the first year a car was made, which turns out to be a question without a clear answer). For a representative for class C_y, simply pick any car that was manufactured in year y.

3.33 (a) It is straightforward to prove that B is symmetric, reflexive, and transitive, so it is an equivalence relation. (b) It is not. It is no anti-symmetric. (c) Let B_i be the positive integers that have i ones in their binary representation. It is easy to see that $B_i \cap B_j = \emptyset$ if $i \neq j$ and that $\mathbb{Z}^+ = B_1 \cup B_2 \cup B_3 \cup \cdots$, so this definition gives us a partition of $\mathbb{Z}^+$. (d) We just let a_i be the number whose binary representation is i 1s. For instance, $a_1 = 1$, $a_2 = 3$, $a_3 = 7$, etc. Notice that we can do better by defining it explicitly: $a_i = 2^i - 1$. (e) The smallest elements of B_2 would be $3 = 11_2$, $5 = 101_2$, $6 = 110_2$, and $9 = 1001_2$. There are infinitely many other possible answers.

4.1 $x_1 = 3-2 = 1$, $x_2 = 3^2 - 2^2 = 5$, $x_3 = 3^3 - 2^3 = 19$, $x_4 = 3^4 - 2^4 = 65$, and $x_5 = 3^5 - 2^5 = 211$.

4.2 It means to find an explicit formula (or closed formula) for it. In other words, a formula that is not recursively defined.

4.3 $x_2 = 2x_1 + 3 = 2 \cdot 1 + 3 = 5$, $x_3 = 2x_2 + 3 = 2 \cdot 5 + 3 = 13$, $x_4 = 2x_3 + 3 = 2 \cdot 13 + 3 = 29$, and $x_5 = 2x_4 + 3 = 2 \cdot 29 + 3 = 61$.

4.4 (a) $x_2 = x_1 + 3 = 2 + 3 = 5$, $x_3 = x_2 + 3 = 5 + 3 = 8$, $x_4 = x_3 + 3 = 8 + 3 = 11$, and $x_5 = x_4 + 3 = 11 + 3 = 14$. (b) $x_n = 3n - 1$. (c) Notice that if $x_n = 3n - 1$, then $x_{n-1} = 3(n-1) - 1 = 3n - 4$. So $x_{n-1} + 3 = 3n - 4 + 3 = 3n - 1 = x_n$, verifying that it works for the recurrence relation. But we also need to show that it works for the base case: $x_1 = 2 = 3(1) - 1$, so it also works for the base case and we are done.

4.5 They are sometimes monotonic. If $r < 0$ they will not be monotonic, but if $r > 0$ they are monotonic. They are also sometimes increasing. For instance, if $r > 1$, it will be increasing, but if $0 < r < 1$ it will be decreasing. If $r < 0$, they are neither increasing nor decreasing since they go back and forth between positive and negative.

4.6 They are always monotonic. A given arithmetic progression is either always increasing or always decreasing, depending on whether d is positive or negative.

4.7 Many answers are possible, but your answer should be very similar in form as the ones given. (a) $a_n = 3(2/3)^n$. (b) $b_n = 2 + 8n$. (c) $c_n = (5/3)c_{n-1}$, $c_0 = 3$. (d) $d_n = d_{n-1} + 9/4$, $d_0 = 8$.

4.8 They are not because $-x^i = -(x^i)$ and $(-x)^i = (-1)^i(x)^i$. Depending on whether x is positive or negative and depending on whether i is even or odd, these may have opposite signs.

4.9 $\displaystyle\sum_{i=0}^{6} -(-3)^i$ or $\displaystyle\sum_{i=0}^{6}(-1)^{i+1}3^i$.

4.10 $$\sum_{k=0}^{30} 5k - 7 = \sum_{k=0}^{30} 5k - \sum_{k=0}^{30} 7 = 5\sum_{k=0}^{30} k - 7 * 31 = 5\frac{30 \cdot 31}{2} - 217 = 2108$$

4.11 $$\sum_{k=0}^{n} 2^k = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1 \text{ or } \sum_{k=0}^{n} 2^k = \frac{1 - 2^{n+1}}{1 - 2} = \frac{1 - 2^{n+1}}{-1} = 2^{n+1} - 1.$$

4.12 Sure. Whenever $x_0 = 0$.

4.13 If you can get this one without mistakes, you are doing *really* well! If you don't quite get it, keep trying to do it on your own. You will learn a lot in the process and it will be a good algebra refresher.

$$\sum_{k=1}^{23} \frac{11}{(-7)^k} = 11\sum_{k=1}^{23} \frac{1}{(-7)^k} = 11\sum_{k=1}^{23} \left(\frac{1}{-7}\right)^k = 11\sum_{k=1}^{23} \left(-\frac{1}{7}\right)^k = 11\left(\sum_{k=0}^{23} \left(-\frac{1}{7}\right)^k - \left(-\frac{1}{7}\right)^0\right)$$
$$= 11\left(\frac{1 - \left(-\frac{1}{7}\right)^{24}}{1 - \left(-\frac{1}{7}\right)} - 1\right) = 11\left(\frac{1 - (-1)^{24}\left(\frac{1}{7}\right)^{24}}{\frac{8}{7}} - 1\right) = 11\left(\frac{7}{8}\left(1 - \left(\frac{1}{7}\right)^{24}\right) - 1\right)$$
$$= 11\left(\frac{7}{8} - \frac{7}{8}\left(\frac{1}{7}\right)^{24} - 1\right) = 11\left(-\frac{1}{8} - \frac{1}{8}\left(\frac{1}{7}\right)^{23}\right) = -\frac{11}{8}\left(1 + \left(\frac{1}{7}\right)^{23}\right).$$

4.14 According to Theorem 4.84, $\cos x = 1 - \dfrac{x^2}{2!} + \dfrac{x^4}{4!} - \cdots + (-1)^n \dfrac{x^{2n}}{(2n)!} + \cdots$. To approximate $\cos(1)$, we can just use several terms of the infinite sum. So,

$$\cos(1) \approx 1 - \frac{1^2}{2!} + \frac{1^4}{4!} - \frac{1^6}{6!} = 1 - \frac{1}{2} + \frac{1}{24} - \frac{1}{720} = \frac{720 - 360 + 30 - 1}{720} = \frac{389}{720} \approx 0.540277.$$

Note that $\cos(1) = 0.540302305\cdots$, so our approximation is pretty good.

4.15 No. You can only add matrices that have the same dimensions (number of rows and columns).

4.16 $A = \begin{bmatrix} 1 & 3 & 9 \\ 2 & 6 & 18 \\ 4 & 12 & 36 \\ 8 & 24 & 72 \end{bmatrix}$.

4.17 $3A = \begin{bmatrix} -9 & 0 & 3 \\ 12 & -6 & 15 \end{bmatrix}$ $A - B = \begin{bmatrix} -4 & -7 & 6 \\ -3 & -3 & -3 \end{bmatrix}$.

4.18 $\mathbf{0}_{3\times 4} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ and $\mathbf{I}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

4.19 In the first case you can since the number of columns of the first matrix is equal to the number or rows of the second one. The result will have dimension 3×7. In the second case you cannot do the multiplication since $3 \neq 6$. That is, the number of columns of the first is not the same as the number or rows of the second.

4.20 $\begin{bmatrix} 2 & 2 \\ 0 & -2 \end{bmatrix}$

4.21 $A^{19} = A^5 A^{14} = \mathbf{0}_n A^{14} = \mathbf{0}_n$.

4.22 Observe that

$$\begin{bmatrix} -4 & x \\ -x & 4 \end{bmatrix}^2 = \begin{bmatrix} -4 & x \\ -x & 4 \end{bmatrix} \begin{bmatrix} -4 & x \\ -x & 4 \end{bmatrix} = \begin{bmatrix} 16 - x^2 & 0 \\ 0 & 16 - x^2 \end{bmatrix},$$

and so we must have $16 - x^2 = -1$ which gives us $x = \pm\sqrt{17}$.

4.23 Disprove! Take for example $A = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$. Then

$$A^2 - B^2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} -1 & 0 \\ -2 & 1 \end{bmatrix} = (A + B)(A - B).$$

4.24 Disprove! This is not generally true. Take $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$. Clearly $A^T = A$ and $B^T = B$. We have

$$AB = \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix}$$

but

$$(AB)^T = \begin{bmatrix} 3 & 3 \\ 1 & 2 \end{bmatrix}.$$

4.25 Disprove! Take $A = B = \mathbf{I}_n$ for any $n > 1$. Then $\operatorname{tr}(AB) = n < n^2 = \operatorname{tr}(A)\operatorname{tr}(B)$.

4.26 We have

$$(AA^T)^T = (A^T)^T A^T = AA^T.$$

5.1 $f(n) = O(g(n))$ means that $f(n)$ grows no faster than $g(n)$. Another way of phrasing it is saying that $g(n)$ is an upper bound on $f(n)$. *If you said that it means $g(n)$ grows faster than $f(n)$, you are not quite correct. Go reread the definition and make sure you are clear on this point!* $f(n) = \Theta(g(n))$ means that $f(n)$ and $g(n)$ grow at the same rate. Another way of phrasing it is saying that $g(n)$ is a tight bound on $f(n)$.

5.2 (a) No. It means there is some n_0 such that whenever $n \geq n_0$, $f(n) \leq cg(n)$ (where $c > 0$ is some constant). So there are two problems with saying it means $f(n) \leq g(n)$. First, there is a constant involved. So $f(n) \leq c\,g(n)$, not just $f(n) \leq g(n)$. Second, it does not have to hold for all values of n, but only for (i.e. $n \geq n_0$). (b) No. Repeating what was said in the previous part, it has to hold for all values of n at least as large as some given value n_0, but it does not have to hold for smaller values of n. (c) That is certainly possible. For instance, if $f(n) = 100n$ and $g(n) = n^2$, $g(10) = 100 < 1000 = f(10)$, but hopefully it is clear that $f(n) = O(g(n))$.

5.3 No. For instance, if $f(n) = 23n$ and $g(n) = n^2$, then $f(n) = O(g(n))$, but $f(n) \neq \Theta(g(n))$.

5.4 Yes. $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. So if $f(n) = \Theta(g(n))$, then $f(n) = O(g(n))$.

5.5 If $f(n) = o(g(n))$, then we know that $f(n)$ grows *slower than* $g(n)$. If $f(n) = O(g(n))$, then $f(n)$ grows *no faster than* $g(n)$. That is, $f(n)$ either grows slower than $g(n)$ or they grow at the same rate.

5.6 More. If you know that $f(n) = \Theta(g(n))$, then you know that they grow at the same rate. But if you only know that $f(n) = O(g(n))$, it is possible that the grow at the same rate, but it is also possible that $f(n)$ grows slower than $g(n)$.

5.7 Proof 1: Notice that if $n \geq 1$, $7n^3 + 4n^2 - 8n + 27 \leq 7n^3 + 4n^2 + 27 \leq 7n^3 + 4n^3 + 27n^3 = 38n^3$. By definition of Big-O, $7n^3 + 4n^2 - 8n + 27 = O(n^3)$.

Proof 2: Notice that $\lim_{n\to\infty} \dfrac{7n^3 + 4n^2 - 8n + 27}{n^3} = \lim_{n\to\infty} \dfrac{7n^3}{n^3} + \dfrac{4n^2}{n^3} - \dfrac{8n}{n^3} + \dfrac{27}{n^3} = \lim_{n\to\infty} 7 + \dfrac{4}{n} - \dfrac{8}{n^2} + \dfrac{27}{n^3} = 7 + 0 + 0 + 0 = 7$. Thus, $7n^3 + 4n^2 - 8n + 27 = \Theta(n^3)$ by Theorem 5.50 (part 3). By Theorem 5.18, $7n^3 + 4n^2 - 8n + 27 = O(n^3)$.

5.8 Notice that $\lim_{n\to\infty} \dfrac{3^n}{3.1^n} = \lim_{n\to\infty} \left(\dfrac{3}{3.1}\right)^n = 0$ since $\frac{3}{3.1} < 1$. By Theorem 5.50 (part 1), $3^n = o(3.1^n)$.

5.9 Notice that both functions have a factor of n. Since $\log n$ grows faster than c (which doesn't grow at all since it is a constant), $n \log n$ grows faster than cn.

It is actually easy to prove this formally: $\lim_{n\to\infty} \dfrac{n \log n}{c\,n} = \lim_{n\to\infty} \dfrac{\log n}{c} = \infty$, so by Theorem 5.50, $n \log n = \omega(cn)$. In other words, $n \log n$ grows faster than cn.

5.10 No! The function may grow slowly, but *it is still growing.* So you are multiplying a function by another function that is growing (even if slowly), which grows faster than 1. Thus, $f(n) \log n$ definitely grows faster than $f(n)$.

As with the previous question, a simple limit computation gives a clear proof of this fact. $\lim_{n\to\infty} \dfrac{f(n) \log n}{f(n)} = \lim_{n\to\infty} \dfrac{\log n}{1} = \infty$, so by Theorem 5.50, $f(n) \log n = \omega(f(n))$. In other words, $f(n) \log n$ grows faster than $f(n)$.

5.11 8675309, $7 \log_{10} n \sim \log_3 n$, $27n$, $7n \log_2 n$, $n^2 + n + 1 \sim 3n^2$, $n^3 \sim n^3 + n^2 \log_e n$, 2^n, 7^n, $n!$, n^n

5.12 We need a "starting point." Induction proofs involve proving a statement of the form $P(k) \to P(k+1)$. That is, we prove that if P is true for some value, then it is true for the next value. But that does not imply that it is ever true–only that if it is true for some value, it is true for the next value. So we need to prove that P is true for some value to get things started.

5.13 This is not circular reasoning because we are not proving that $P(k+1)$ is true. We are proving that $P(k) \rightarrow P(k+1)$ is true. In other words we are assuming $P(k)$ is true, and the using that fact to prove that $P(k+1)$, which is a *different* statement, is true. But again, we did not prove that $P(k+1)$ is *always* true. We only proved that *IF* $P(k)$ is true, then $P(k+1)$ is true.
5.14 (a) It is saying that if $P(a)$ is true and it is also true that whenever $P(k)$ is true that $P(k+1)$ is true, then $P(n)$ is true for all $n \geq a$. (b) We know that $P(a)$ is true. We also know that $P(k) \rightarrow P(k+1)$ is true for all $k \geq a$. In particular, we know that $P(a) \rightarrow P(a+1)$ is true. Using modus ponens, we can conclude that $P(a+1)$ is true. But then we can use modus ponens again to conclude that $P(a+2)$ is true (since we know $P(a+1)$ and $P(a+1) \rightarrow P(a+2)$ are both true). We can keep doing this over and over again so that eventually we can show that $P(a+k)$ is true for any $k \geq 0$. Thus, $P(n)$ is true for all $n \geq a$.
5.15 No. Notice that we know that $P(0)$ is true, but we only know that $P(k) \rightarrow P(k+1)$ for $k > 0$. So we know $P(1) \rightarrow P(2)$, but we do not know whether or not $P(0) \rightarrow P(1)$. In other words, we have a base case and an inductive case, but the inductive case does not go all the way down to the base case, so we cannot connect them. (Note: this is not a failure of induction. It is a failure in trying to use induction. A proper induction proof would show that $P(k) \rightarrow P(k+1)$ for $k \geq 0$ so that the inductive step applies to the base case.)
5.16 There are clearly $2 = 2^1$ binary strings of length 1 ('0' and '1'). Assume that there are 2^k binary strings of length k. Every string of length $k+1$ ends with either a '0' or a '1', and the first k characters can be any of the possible binary strings of length k. In other words, the number of binary strings of length $k+1$ is $2 \cdot 2^k = 2^{k+1}$ since we can append to each of the 2^k strings of length k either a '0' (producing 2^k strings of length $k+1$) or a '1' (producing a different 2^k strings of length k). Since we proved the base and inductive cases, we have shown that the number of binary strings of length k is 2^k.
5.17 These are both correct techniques.
5.18 In weak induction you assume P is true for a given value and show P is true for the next value. For instance, you might assume $P(k)$ is true and prove that $P(k+1)$ is true. In strong induction you assume that P is true for every value from the base case up to a certain value, and then you prove it for the next value. For instance, you assume $P(1) \wedge P(2) \wedge \cdots \wedge P(k-1)$ is true and prove that $P(k)$ is true. (By the way, I purposely used $P(k)$ and $P(k+1)$ for one and $P(k-1)$ and $P(k)$ for the other to re-emphasize that you can do it either way.)
5.19 Induction is like a bunch of dominoes lined up. If you push the first one over, it will push the next one over, which will push the next one over, etc., until they have all fallen down. The first domino is the base case. The fact that the dominoes are placed close enough to each other is like the inductive case (because they are close enough, if one falls, the next one will).
5.20 A recurrence relation is a recursively defined formula for the values of a sequence. In other words, it is a formula to compute a_n based on one or more values of a_i where $i < n$.
5.21 It means to come up with a closed formula. That is, formula to compute the nth term of the sequence directly (not based on previous values of the sequence).
5.22 (a) The substitution method essentially involves guessing the correct formula and using induction to prove it. (b) The iteration method keeps applying the recursive definition to the right side of the formula until it can be simplified down to (generally speaking) a summation and the base case(s) that is then simplified. (c) To use the Master Theorem, one verifying that the recurrence relation is in the correct form, identifies the constants from the theorem (a, b, and d), determines which case the formula falls into based on the values of the constants, and writes down the answer based on which case it is. This technique only gives an asymptotic bound on the solution, not an exact solution.
5.23 (a) They both give an exact formula whereas the Master Theorem only gives an asymptotic

bound. (b) The Master Method is *much easier* to use than the other two techniques. (c) You need to be able to determine the answer before you prove it. If the formula is complicated, you may not be able to determine what it is. (d) The main downside is that it is messy. It also only works well on simple recurrence relations. For instance, if a recurrence relation has several recursive terms (e.g. $T(n) = T(n-1) - 2T(n-3)$), it would probably be quite complicated to try to solve it using iteration. (e) The Master Theorem also only works on one specific type of recurrence relation and it does not give an exact solution. (f) If I don't care about an exact solution, the Master Theorem is by far the easiest, so I would use that one. If I want an exact solution, I would prefer substitution if I can see an obvious pattern and find the formula. If I can't find a formula, I would prefer iteration because I should be able to work it out using that technique.

5.24 Because the three topics have a lot in common. Recurrence relations are just a form of recursion, and they can be solved using induction.

6.1 Answers will vary, but here are a few examples. (a) I want to adopt a dog. At the pet shop, there are four golden retrievers, two poodles and 5 corgis. How many choices do I have if I plan to adopt one dog? You can choose either a golden retriever (4 options), a poodle (2 options), or a corgi (5 options). So the total number of choices is $4 + 2 + 5 = 11$.

(b) I go to a restaurant and see that there are 15 dessert choices, 10 main courses, and 2 appetizers. How many choices do I have if I want to order one of each? You have 15 choices for desserts, and independent of that you have 10 choices for a main course, and independent of both of those you can choose one of two appetizers. So you have $15 * 10 * 2 = 300$ choices.

(c) Your password can be from 4 to 8 lower case alphabetic characters. How many possibilities are there? There are 26 possible characters. If you use 4 characters, there are $26 \times 26 \times 26 \times 26 = 26^4$ possible passwords. Similarly, with 5 characters there are 26^5 possible passwords. Likewise, for 6, 7, and 8 characters, there are 26^6, 26^7, and 26^8 possible passwords. Since you have to choose one of these lengths, the total number of possible passwords is $26^4 + 26^5 + 26^6 + 26^7 + 26^8$.

6.2 You cannot conclude that a box has at least 3 objects, that two boxes have at least two items, or that every box has at least one item. (For each of these you can come up with a distribution of objects in boxes that does not fit the description.) The most you can conclude is that at least one box has at least 2 objects.

6.3 You might have all 30 balls in one bin. You might have 15 balls in one bin, and 15 in a second bin. You might have 1 balls in each of the first 6 bins and 24 in the 7th bin. You might have 4 balls in each of the first 6 bins and 6 balls in the 7th bin. You might have 4 balls in each of the first 5 bins, and 5 balls in each of the final two bins. Notice that in all of these examples, there is at least one box which has at least $\lceil 30/7 \rceil = 5$ balls as guaranteed by the generalized pigeonhole principle.

6.4 There are 4 types of discs. Therefore by the generalized pigeonhole principle, I know that I have at least $\lceil 21/4 \rceil = 6$ discs of at least one type. But that is all I can say. I do not know which type I have at least 6 of. For instance, it is possible all 21 are putter, or all 21 are distance drivers, for instance, so I do not even know if I have a single disc of any type.

6.5 The numbers between 1 and 1000 can all be represented with 10 bits. A number between 1 and 1000 can have between 1 and 10 bits that are 1s. So the 12 numbers can each be placed in one of 10 "bins" based on how many bits they have in their binary representation. Since we are placing 12 numbers in 10 bins, at least one bin has at least 2 numbers. In other words, two of the numbers have the same number of 1s in their binary representation. (None of the numbers can actually have 10 1s because the number with 10 1s is 1023 which is larger than 1000. So technically there are only 9 bins. But the argument is the same either way. However, if I said that ten people picked numbers, then we would need to take this into account to solve the problem correctly.)

6.6 Permutations are ordered and combinations are not. More specifically, a permutation is a reordering of objects, whereas a combination is a selection of objects. They are basically completely

different things.

6.7 (a) $10 \cdot 10 \cdot 10 = 10^3 = 1000$ (assuming you regard $0 = 000$, $12 = 012$, etc. as 3 digit numbers). (b) $10 \cdot 9 \cdot 8 = 720$. (c) Because sets cannot have repeats, there are $\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$. *Notice that there are 6 times as many three-digit numbers with no repeated digits than sets of three digits because each set with three digits leads to 6 different three-digit numbers (e.g. the set $\{1, 2, 3\}$ is the same as the set $\{3, 1, 2\}$, for instance, but the numbers 123, 132, 213, 231, 312, 321 are all different.)* (d) Because lists can have repeats, there are $10 \cdot 10 \cdot 10 = 10^3 = 1000$.

6.8 (a) 7!. (b) 5!.

6.9 Using Theorem 6.49, there are $\frac{5!}{2! \cdot 2! \cdot 1!} = \frac{120}{4} = 30$.

6.10 Choose 5 people who are *not* on the team.

6.11 $\binom{25}{22} = \binom{25}{3} = \frac{25 \cdot 24 \cdot 23}{3 \cdot 2 \cdot 1} = \frac{25 \cdot (6 \cdot 4) \cdot 23}{6} = 25 \cdot 4 \cdot 23 = 2300$.

6.12 (a) $\binom{11}{4}$. (b) 4!. (c) We can choose the 4 members ($\binom{11}{4}$ ways) and then place them into the offices (i.e. order them, so 4! ways) for a total of $\binom{11}{4} \cdot 4! = 11 \cdot 10 \cdot 9 \cdot 8 = 7920$ ways. Alternatively, we have 11 choices for president, and once the president has been decided there are not 10 choices for vice-president, then 9 for treasurer, and finally 8 for secretary, for a total of $11 \cdot 10 \cdot 9 \cdot 8 = 7920$ ways of choosing.

6.13 Whether or not order matters, whether or not there are repetitions, whether or not objects are distinguishable or not.

6.14 (a) $\displaystyle\sum_{k=0}^{n} \binom{n}{k} 10^k = \sum_{k=0}^{n} \binom{n}{k} 10^k 1^{n-k} = (10+1)^n = 11^n$. (b) $11^0 = 1, 11^1 = 11, 11^2 = 121, 11^3 = 1331, 11^4 = 14641, 11^5 = 161051$. (c) The rows of Pascal's triangle look kind of like the powers of 11. When the numbers in the triangle are longer than 1 digit, you have to actually line them up and add them to get the correct result. But the connection is more clear when you consider the formula for the Binomial Theorem and think about what it says about a row of the triangle.

6.15 Plugging in $2x$ and $-3y$ into the formula, we obtain

$$\begin{aligned}(2x-3y)^5 &= \binom{5}{0}(2x)^0(-3y)^5 + \binom{5}{1}(2x)^1(-3y)^4 + \binom{5}{2}(2x)^2(-3y)^3 + \binom{5}{3}(2x)^3(-3y)^2 \\ &\quad + \binom{5}{4}(2x)^4(-3y)^1 + \binom{5}{5}(2x)^5(-3y)^0 \\ &= -243y^5 + 810x\,y^4 - 1080x^2y^4 + 720x^3y^2 - 240x^4y + 32x^5.\end{aligned}$$

Notice that the negative sign goes inside the parentheses so that it is included in the powers, and that the constants are also inside the parentheses so they are included in the powers.

6.16 Notice that $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n$, where the second-to-last step uses the Binomial Theorem.

6.17 Let M be the set of children who took math and C those who took computer science. Notice that $12 - 4 = 8$ children took either math or computer science, Thus, $|M| = 6$, $|C| = 5$, and $|M \cup C| = 8$. Therefore, it must be that $|M \cap C| = 6 + 5 - 8 = 3$ children took both.

6.18 It is possible that the 4 students who sleep were also late, in which case 13 students did neither. On the other extreme, the 4 students who slept are all different than the 7 who came late. In that case there are 9 students who did neither. So at least 9 and at most 13 students did neither.

6.19 No. There are 7 things on the right side of the equation, so if you only have 6 pieces of information you cannot fully solve the problem.

6.20 $|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D|$
$-|A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D|$
$+|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|$
$-|A \cap B \cap C \cap D|$

7.1 (a) answers will vary. Your graph should have numbers (weights) on every edge, no arrows on the edges, and can contain loops (edges from a vertex to itself). (b) answers will vary. You graph should not have any numbers on the edges, the edges should have arrows, and there may be repeated edges–that is, there might be two different edges from some vertex u to another vertex v. (c) answers will vary. A network is just a weighted directed graph. So your graph should have numbers on the edges and every edge should have an arrow. It should not have loops or repeated edges.

7.2 (a) A road system, where the vertices are intersections and the edges are the segments of road between intersections. The weights on the edges might be distances, speed limits, expected time to traverse, etc. (b) A ski trail map, where the vertices are intersections and the edges are the segments of trail between intersections. The edges are directed because on som trails you are only allowed to go one direction. Since sometimes a trail splits and comes back together, multiple edges are allowed between vertices. The weights can be distances or difficulty ratings. (c) Representing connections on a social media app, where it is assumed that being connected is two-way (e.g. on Facebook when you are friends versus on Instagram where following is one-way), and where you are allows to connect to yourself (I actually do not know of a social media site that allows this, but I suppose it is possible).

7.3 The easiest proof is to realize that edges are just pairs of vertices. There are n vertices. How many ways are there of choosing pairs of vertices? You are choosing 2 things out of n things, so $\binom{n}{2}$.

Here is a proof by induction: A graph with 2 vertices has $1 = \binom{2}{2}$ possible edge, so it holds for the base case (We could use 1 vertex as a base case, but it is more confusing so we start at 2). Assume a graph with $k-1$ vertices, where $k \geq 3$ has $\binom{k-1}{2}$ possible edges. If you add a vertex, it can be connected to each of the $k-1$ vertices, so a graph with k vertices has $\binom{k-1}{2} + (k-1) = \frac{(k-1)(k-2)}{2} + (k-1) = (k-1)\left(\frac{k-2}{2} + 1\right) = (k-1)\left(\frac{k-2+2}{2}\right) = \frac{(k-1)(k)}{2} = \binom{k}{2}$ possible edges. Since the formula is true for $k = 2$, and whenever it is true for $k-1$ it is true for k, it is true for all $n \geq 2$ by induction.

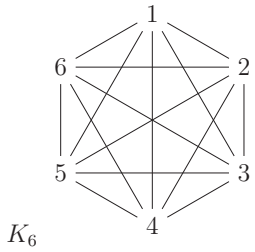
7.4 answers will vary, but here are two examples: $\square|$ or $\boxtimes\wedge$.

7.5 (a) $n-1$. (b) Clearly a tree with 2 vertices has $2-1=1$ edges. Assume all trees with $n-1$ vertices have $n-2$ edges. Let T be a tree with $n > 2$ vertices. Since it is a tree, it contains at least one vertex v of degree 1. Let T' be the tree T with vertex v deleted. Then T' has $n-1$ vertices and is clearly still a tree since removing a vertex of degree 1 cannot either add a cycle or disconnect the graph. Thus T' has $n-2$ edges. But it was created from T by removing a single vertex and edge. Therefore T has $n-1$ edges. Since the formula holds for $n = 2$ and whenever it holds for $n-1$ it holds for n, every tree with $n \geq 2$ vertices has $n-1$ edges.

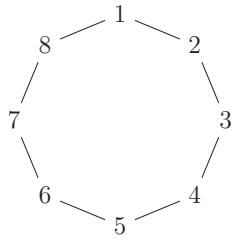
7.6 (a) unweighted. (b) undirected. (c) e and x are not adjacent, but f and b are adjacent. (d) L is connected. (e) 8. (f) 17. (g) $\deg(v) = 2$ and $\deg(c) = 5$. (h) 34. It is twice the number of edges which makes sense because of the Handshaking Lemma. (i) answers will vary, but if you drew a subgraph of L that contains exactly 7 edges and contains no cycles, then it is a spanning tree. Of course it cannot contain cycles because it is a tree. (j) If you remove (e, v) and (f, v), then v is disconnected from the rest of the graph. No single edge will disconnect the graph so 2 edges is the minimum number. (k) answers will vary, but mine are efv, $bcdf$, $abcdx$, $axdfve$, $aefbcdx$, and finally $aevfbcdx$. Notice in all of these, the vertices listed next to each other are adjacent and the

first and last one on the list are adjacent.

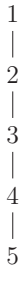
7.7 Here are the graphs for the next 3 questions. The vertices labels are optional.



K_6



C_8



P_5

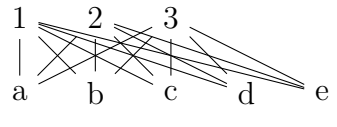
7.8 See above.

7.9 See above.

7.10 Notice to draw Q_2, you can draw two copies of Q_1 (i.e. two lines) and connect corresponding vertices (i.e. if you draw the two lines vertically, connect the top vertices and the bottom vertices) to make a square (notice that Q_2 is the same as C_4). To draw Q_3 (a cube), you can draw two copies of Q_2 (squares) and connect corresponding vertices. Using the same idea, to draw Q_5, I would draw 2 copies of Q_4, and then connect corresponding vertices between the two copies.

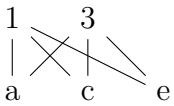
7.11 Notice that two vertices are adjacent iff they differ by exactly 1 bit. Also notice that if two numbers have the same parity, they cannot differ by exactly 1 bit. So we can pick $V_1 = \{000, 011, 101, 110\}$, and $V_2 = \{001, 010, 101, 111\}$. The numbers in V_1 have even parity, and the numbers in V_2 have odd parity. So within each subset, none of the numbers differ by exactly one bit since all of the numbers in each set have the same parity. Thus, this is a valid partition.

7.12 Here is $K_{3,5}$ and one possible subgraph.



$K_{3,5}$

a subgraph of $K_{3,5}$



7.13 Every edge has two endpoints. Each endpoint adds one to the degree of the vertex it is incident with. So if you sum the degree of all of the vertices, it should be twice the number of edges.

7.14 This is a simple application of the Handshaking Lemma. We create a graph as follows: People are vertices, and there is an edge between two people if they have shaken hands. So the statement would imply that in the graph there are an odd number of vertices of odd degree. This contradicts Corollary 7.51 (which is a corollary of the Handshaking Lemma). Thus, the friend is incorrect.

7.15 (a) Recall that an adjacency list requires on the order of $\Theta(n+m)$ memory, whereas for the adjacency matrix it would be $\Theta(n^2)$. If the graph has few edges, then m is much smaller than n^2, so $\Theta(n+m)$ would be smaller and the adjacency list would be appropriate. (b) If the number of edges is larger, then either might be appropriate, depending on how large. If $m \approx n^2$, then we are comparing $\Theta(n+m) = \Theta(n+n^2) = \Theta(n^2)$ with $\Theta(n^2)$, so there is minimal difference between the two. But if m is large but smaller than n^2, the adjacency list might be the better choice.

7.16 If you are storing small graph (e.g. hundreds of vertices or less), it probably does not matter a whole lot. But imagine storing the Facebook friendship graph. As of 2021, there are 2.85 billion Facebook users and each has an average of 350 friends (as of 2019 it was about 338, so this number should be close). Since we are talking about exact numbers, we will compare without using Θ notation. Recall that an adjacency list takes $\Theta(n+m)$ space and an adjacency matrix takes $\Theta(n^2)$ time. We will just treat these as $n+m$ and n^2. In our example, $n = 2,850,000,000$, and $m = 2,850,000,000 * 350 = 997,500,000,000$. So an adjacency list would take about $n + m = 2,850,000,000 + 997,500,000,000 = 1,000,350,000,000$ space. An adjacency matrix would

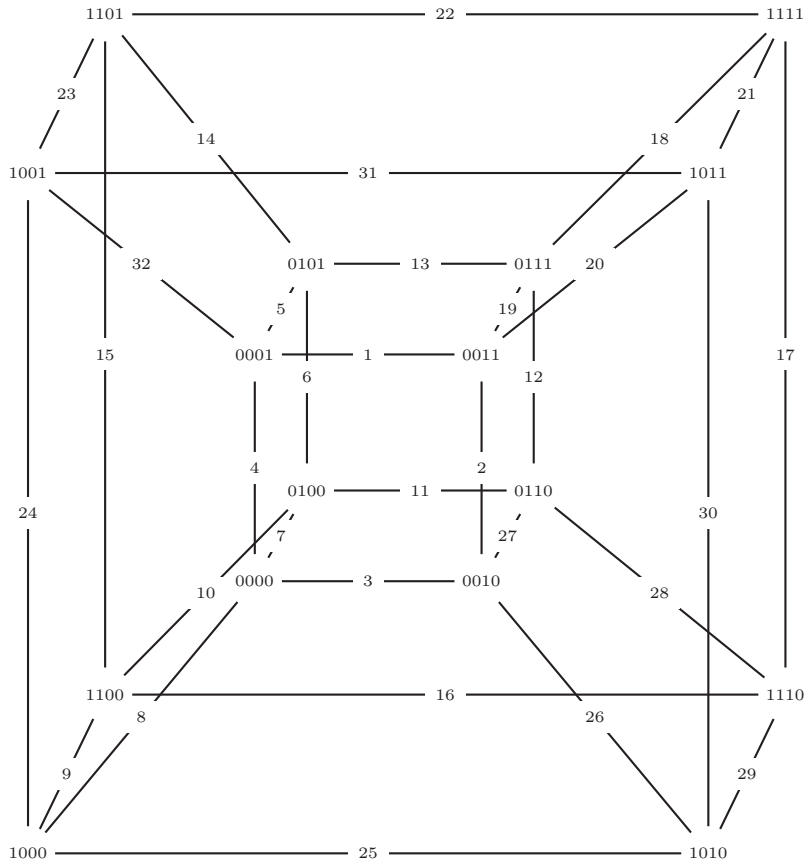
take about $n^2 = 2,850,000,000^2 = 8,122,500,000,000,000,000$ space. In case it isn't clear, the adjacency matrix takes about 8,119,658 times as much space! To be more precise, assuming it takes 32 bits to store each number in an adjacency list or matrix (and that is pushing it), the adjacency list requires about 4 TB (terabtyes) of space, which is doable if you want to fill up the majority of the hard drive on a very new top-of-the-line computer. On the other hand, the adjacency matrix requires about 32.49 EB (exabytes). The largest hard drive you can currently buy is about 18 TB, so you would need about 1,804,369 hard drives to store the adjacency matrix. (Even if you encoded the matrix densely, using only 1 bit per entry, it would still require about 56,387 hard drives.) So yes, it does matter.

7.17 (a) Arbitrarily pick either u or v and check its list for the other–we will look at u's list. Since it might have to traverse the entire list of the neighbors of u, it would be $O(\deg(u))$, which might be as large as $n-1$. So $O(n)$ in the worst case (although $O(\deg(u))$ is more precise). I use big-O notation on this one because it is possible it finds it sooner. (b) Either $\Theta(\deg(u))$ if it has to traverse the list and count, or $\Theta(1)$ if this is maintained in the data structure. (c) $\Theta(\deg(u)) = \Theta(k)$.

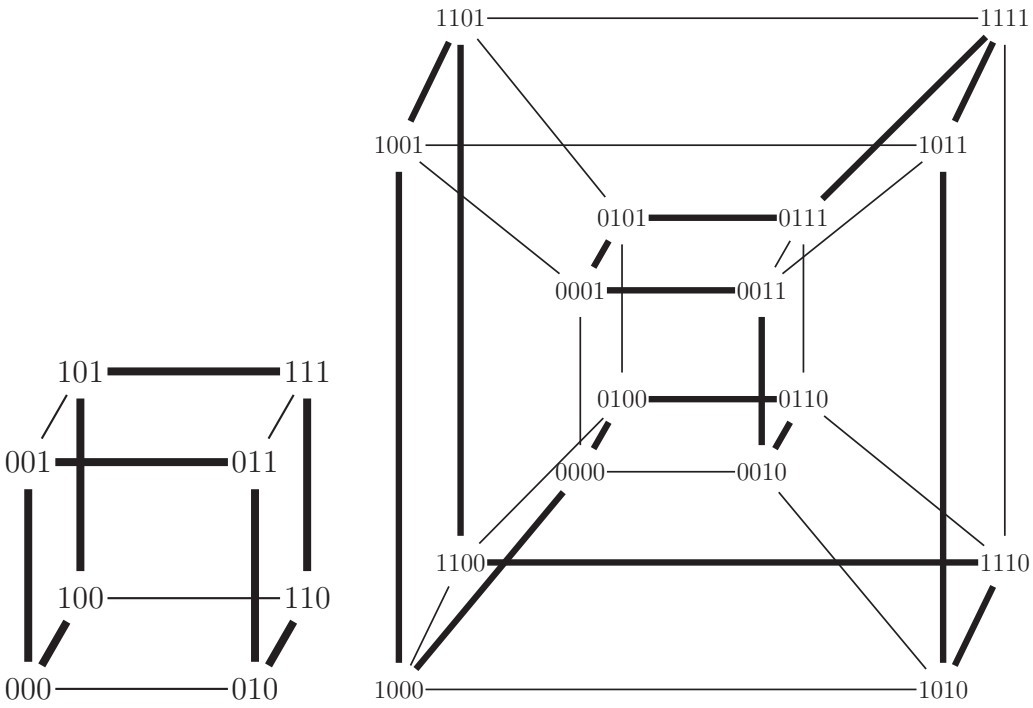
7.18 (a) $\Theta(1)$ since it can just look at the (u, v) entry of the matrix. (b) $\Theta(n)$ since it has to look through an entire row of the matrix to determine which vertices are neighbors. (c) Same answer and reason as (b).

7.19 (a) Either one works fine, but it is more efficient with an adjacency matrix since an edge (u, v) can be added and removed in constant time by just changing the matrix entry (u, v) to a 0 or 1. For an adjacency list, to remove (u, v), you would have to find u on v's list and v on u's list and then remove them from the lists, so it would take longer. (b) Adjacency list by far. If you add a vertex, you can just add an adjacency list for it to your current list. With a matrix, you need to create an entirely new matrix with one more row and column and copy all of the entries, so it is not very efficient. Similar problems exist when removing vertices.

7.20 (a) Since every vertex of K_5 has degree 4, it is Eulerian by Theorem 7.69. (b) Since every vertex of K_6 has degree 5, it is *not* Eulerian by Theorem 7.69. (c) Since every vertex of Q_3 has degree 3, it is *not* Eulerian by Theorem 7.69. (d) Since every vertex of Q_4 has degree 4, it is Eulerian by Theorem 7.69. Here is one of many possible orderings of the edges that form an Eulerian tour:

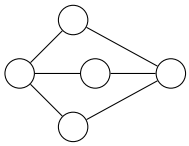


(e) and (f) are both are Hamiltonian. Here is one possible Hamiltonian cycle for each:



(g) Yes. Since it is just a cycle with all of the vertices, it is clearly a Hamiltonian cycle.

7.21 Here is the most obvious way to draw it:

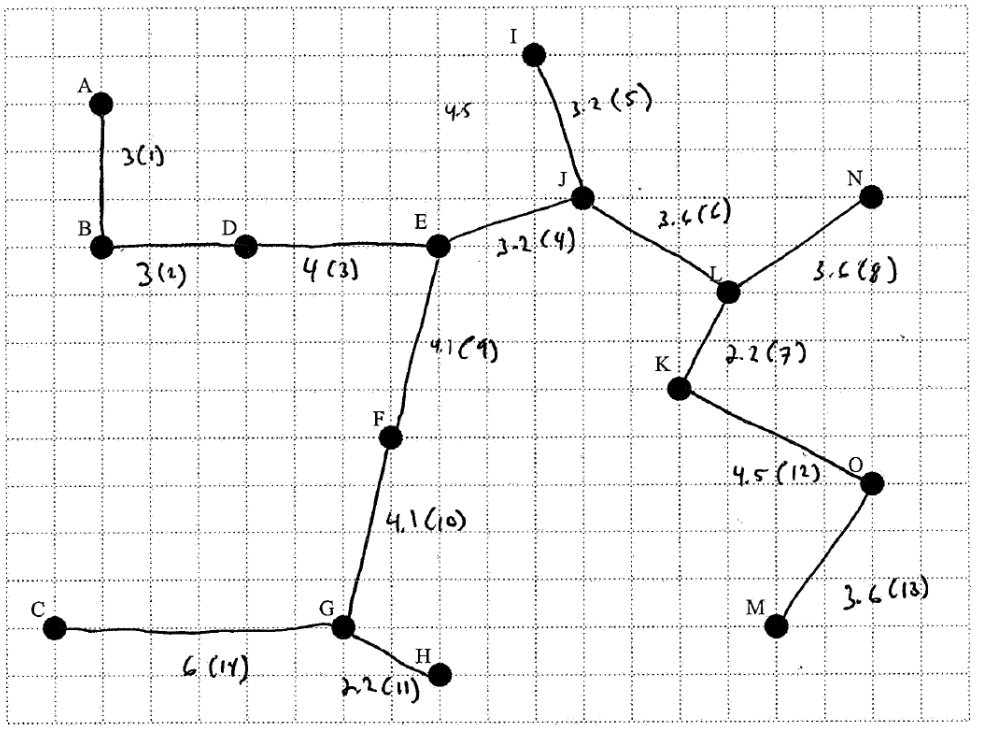


7.22 It is not saying that. No planar graphs have more edges than that, but not every graph with fewer edges is planar. For instance, $K_{3,3}$ has $v = 6$ and $e = 9$. So $e = 9 < 12 = 3v - 6$, but as we saw earlier, $K_{3,3}$ is not planar.

7.23 (a) I am too lazy to do another drawing, but draw it as a box inside a box with the corners connected to each other and it is clearly planar. (b) Notice that $v = 16$, $e = 32$, and C_3 is not a subgraph of Q_4. Then $e = 32 > 28 = 2v - 4$, so by part (b) of Theorem 7.79, Q_4 cannot be planar.

7.24 No. By definition, the one with weight 35 would not be a minimum spanning tree.

7.25 (a) The dots are vertices and we can think of it being a complete graph where the weight of each edge is the distance between the two dots. (b) We want to route to every house, but we want to minimize wire. Thus, a spanning tree makes sense because if we have any cycles, we are wasting wire. Not only that, we want a minimum spanning tree to use the least amount of wire. (c) Prim's algorithm makes the most sense because it is a lot easy to start somewhere and find the closest point to the current partial tree. On the other hand, with Kruskal's algorithm, we would have to sort a list if $\binom{n}{2}$ edges. (d) There is a unique solution with a cost of about 50.3 as shown below.



7.26 (a) (A, D), (A, E), (B, D), and (C, D). (b) (A, E) is the only light edge. (c) (A, D) and (B, D) cross the cut. (d) The path with vertices C, B, A, E, D is a minimum spanning tree of weight 10. (e) The minimum spanning tree is unique because it uses the 4 lightest edges of the graph so there can't be one with smaller weight.

7.27 A graph must have at least some edges of repeated weight in order for there to be multiple minimum spanning trees.

Exercise Solutions

1.3 (a) false. (b) true. (c) false. If you don't know the story behind this, Google it.

1.5 (a) Not a proposition. (b) I would like to think this is true. However, this is not a proposition since not everyone agrees with me. (c) Also not a proposition. (d) true. (e) false. This one is a bit tricky to think about it, so the next example will ask you to prove it.

1.9 "I am not learning discrete mathematics." You could also have "It is not the case that I am learning discrete mathematics," although it is better to smooth out the English when possible.; False. Since you are currently reading the book, you *are* learning discrete mathematics.

1.13 Either "I like cake and I like ice cream," or "I like cake and ice cream" are correct.

1.16 "$x > 0$ or $x < 10$"; true; true; $x < 10$; true.

1.17 (a) "It is not the case that Jill is tall," which is awkward, so could be shorted to "Jill is not tall" or perhaps "Jill is short." (b) "Jill is tall or Jill is smart," or more compactly, "Jill is tall or smart." (c) "Jill is tall and Jill is smart," or more compactly, "Jill is tall and smart." (d) "Jill is tall and Jill is not smart." (e) This one is a bit tricky, and we will see a tool shortly that will make it easier. But for now, hopefully you can see that is would be "it is not the case that Jill is tall and Jill is smart." Notice that an *incorrect* answer would be "Jill is neither tall nor smart." We will see why later.

1.20 (a) XOR; (b) OR. This one is a little tricky because parts can't be simultaneously true so it sounds like an XOR. But since the point of the statement is not to *prevent* both from being true, it is an OR. (c) Without more context, this one is difficult to answer. I would suspect that most of the time this is probably OR. The purpose of this example is to demonstrate that sometimes life contains ambiguities. This is particularly true with software specifications. Generally speaking, you should *not* just assume one of the alternative possibilities. Instead, get the ambiguity clarified. (d) When course prerequisites are involved, OR is almost certainly in mind. (e) The way this is phrased, it is almost certainly an XOR.

1.21 $p \vee q$ is "either list 1 or list 2 is empty." To be completely unambiguous, you could rephrase it as "at least one of list 1 or list 2 is empty." $p \oplus q$ is "either list 1 or list 2 is empty, but not both," or "precisely one of list 1 or list 2 is empty." They are different because if both lists are empty, $p \vee q$ is true, but $p \oplus q$ is false.

1.22 (a) No. If p and q are both true, then $p \vee q$ is true, but $p \oplus q$ is false, so they do not mean the same thing. (b) We have to be very careful here. In general, the answer to this would be absolutely not (we'll discuss this more next). However, for *this particular* p *and* q, they actually essentially are the same. But the reason is that it is impossible for x to be less than 5 and greater than 15 at the same time. In other words, p and q can't both be true at the same time. The only other way for $p \oplus q$ to be false is if both p and q are false, which is exactly when $p \vee q$ is false.

1.26 (a) An A. This is pretty obvious since we earned 94% and if we earn 94%, then we will get an A. (b) We can't be sure. We know that earning 94% is enough for an A, but we don't know whether or not there are other ways of earning an A. (c) We can't be sure. If the premise is false, we don't know anything about conclusion.

1.30 (a) An A. (b) Yes. Because it is a biconditional statement that we assumed to be true, the statements "you will receive an A in the course" and "you earn at least 94%" have the same truth value. Since the former is true, the latter has to be true. (c) Yes. Notice that $p \leftrightarrow q$ is equivalent to $\neg p \leftrightarrow \neg q$ (You should convince yourself that this is true). Thus the statements "you don't earn at least 94%" and "you didn't get an A" have the same truth value.

1.32 The answers are in **bold**.

With Variables/Operators	In English
$p \to q$	**If *Iron Man* is on TV, then I will watch it.**
$\boldsymbol{(\neg r \wedge p) \to q}$	If I don't own *Iron Man* on DVD and it is on TV, I will watch it.
$p \wedge r \wedge \neg q$	***Iron Man* is on TV and I own the DVD, but I won't watch it.**
$\boldsymbol{q \leftrightarrow p}$	I will watch *Iron Man* every time it is on TV, and that is the only time I watch it.
$\boldsymbol{r \to q}$	I will watch *Iron Man* if I own the DVD.

1.35 Here is the truth table with one (optional) intermediate column.

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

1.37 Here is the truth table with two intermediate columns. For consistency, your table should have the rows in the same order.

a	b	c	$\neg b$	$a \vee \neg b$	$(a \vee \neg b) \wedge c)$
T	T	T	F	T	T
T	T	F	F	T	F
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	F	T	T	F

1.40 $(a \wedge b) \vee c$

1.41 They are not equivalent. For instance, when $a = F$, $b = F$, and $c = T$, $(a \wedge b) \vee c$ is true but $a \wedge (b \vee c)$ is false.

1.42 Since $(a \to b) \to c$ is how it should be interpreted, the first statement is correct. The second statement is incorrect. We'll leave it to you to find true values for a, b, and c that result in these two parenthesizations having different truth values.

1.45 (a) tautology (b) contradiction; p and $\neg p$ cannot both be true. (c) contingency; it can be either true or false depending on the truth values of p and q.

1.47

Evaluation of Proof 1: Nice truth table, but what does it *mean*? It is just a bunch of symbols on a page. Why does this truth table prove that the proposition is a tautology? The proof needs to include a sentence or two to make the connection between the truth table and the proposition being a tautology.

Evaluation of Proof 2: This is mostly correct, but the phrasing could be improved. For instance, the phrase 'they all return true' is problematic. Who/what are 'they'? And what does it mean that they 'return' true? Propositions don't 'return' anything. Replace 'Since they all return true' with 'Since every row of the table is true' and the proof would be good.

Evaluation of Proof 3: While I applaud the attempt at completeness, this proof is way too complicated. It is hard to understand because of the incredibly long sentences and the mathematical statements written in English in the middle of sentences. But I suppose that technically speaking it is correct. Here are a few specific examples of problems with the proof (not exhaustive). The first three sentences are confusing as stated. The point that the author is trying to make is that whenever q is true, the statement must be true regardless of the value of p, so there is nothing further to verify. Thus the only case left is when q is false. This point could be made with far few words and more clearly. The phrase 'we would have true and (true implies false), which is false,' is very confusing, as are a few similar statements in the proof. The problem is that the writer is trying to express mathematical statements in sentence form instead of using mathematical notation. There is a reason we learn mathematical notation–to use it!

Evaluation of Proof 4: This proof is correct and is not too difficult to understand. It is a lot better than the previous proof for a few reasons. First of all, it starts off in a better place–focusing in on the single case of importance. Second, it uses the appropriate mathematical notation and refers to definitions and previous facts to clarify the argument.

Evaluation of Proof 5: While I appreciate the patriotism (in case you don't know, some people use 'merica as a shorthand for America), this has nothing to do with the question. Sorry, no points for you! By the way, I did *not* make this solution up. Although it wasn't really used on this particular problem, one student was in the habit of giving answers like this if he didn't know how to do a problem.

1.51 Below is the truth table for $\neg(p \wedge q)$ and $\neg p \vee \neg q$ (the gray columns).

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Since they are the same for every row of the table, $\neg(p \wedge q) = \neg p \vee \neg q$.

1.53

$$\begin{aligned} p &= \underline{p \wedge T} && \text{(identity)} \\ &= \underline{p \wedge (p \vee \neg p)} && \text{(negation)} \\ &= \underline{(p \wedge p) \vee (p \wedge \neg p)} && \text{(distributive)} \\ &= \underline{(p \wedge p) \vee F} && \text{(negation)} \\ &= p \wedge p && \underline{\text{(identity)}} \end{aligned}$$

Thus, $\underline{p \wedge p = p}$.

1.55 (a) We can use the identity, distributive, and dominations laws to see that

$$p \vee (p \wedge q) = (p \wedge T) \vee (p \wedge q) = p \wedge (T \vee q) = p \wedge T = p.$$

(b) We can prove this similarly to the previous one, or we can use the previous one along with distribution and idempotent laws:

$$p \wedge (p \vee q) = (p \wedge p) \vee (p \wedge q) = p \vee (p \wedge q) = p.$$

1.57 (a) $p \oplus q$; (b) $(p \wedge \neg q) \vee (\neg p \wedge q)$ or $(p \vee q) \wedge \neg(p \wedge q)$. Other answers are possible, but most likely you came up with one of these. If not, construct a truth table to determine whether or not your answer is correct.

1.59

Evaluation of Proof 1: This is an incomplete proof. It only proves that in one case (p and q both being true) they are equivalent. It says nothing about, for instance, whether or not they have the same truth value when p is true and q is false.

Evaluation of Proof 2: This proof is also incomplete. It proves that in two cases they have the same truth value, but is silent about the other cases. Are we supposed to *assume* that in all other cases the expressions are both false?

Evaluation of Proof 3: This is either incomplete or incorrect, depending on how you read it. If by "precisely" the writer means "exactly when", then it is incorrect since the propositions are also true when both p and q are false. Otherwise the proof is incomplete because it does not deal with every case.

Evaluation of Proof 4: This is correct because it exhausts all of the cases. It is perhaps a bit brief, however. The only way I know the proof is actually correct is that I have to verify what the writer said. By the definition of $p \leftrightarrow q$, what they said is clearly true. But to see that it is true of $(p \wedge q) \vee (\neg p \wedge \neg q)$ I have to actually plug in a few values and/or think about the meaning of the expression.

1.63 (a) is a predicate since it can be true or false depending on the value of x.; (b) is not a predicate since it is simply a false statement–it doesn't contain any variables.; (c) is a predicate since it can be true or false depending on the value of M.; (d) is not a predicate. This one is tricky. This is a definition. In this statement, x is not a variable but a label for a number so that it can be referred to later in the sentence.

1.67

(a) $\forall x(2x < 3x)$. In case it isn't obvious, there is nothing magical about x. You could also write your answer as $\forall a(2a < 3a)$, for instance.

(b) $\forall n(n! < n^n)$.

1.70 $\forall x \neq 0(x^2 \neq 0)$. Alternatively, $\forall x(x \neq 0 \rightarrow x^2 \neq 0)$.

1.73 $\exists x(x > 0)$.

1.75

Evaluation of Solution 1: While perhaps technically correct, this solution is not very good. It at least uses a quantifier. But the fact that it includes the phrase "is even" suggests that it could be phrased a bit more 'mathematically.'

Evaluation of Solution 2: This solution is pretty good. It is concise, but expresses the idea with mathematical precision. Although it doesn't directly appeal to the definition of even, it does use a fact that we all know to be true of even numbers.

Evaluation of Solution 3: This solution is also good. It clearly uses the definition of even. It is a bit more complicated since it uses two quantifiers, but I prefer this one slightly over the second solution. But that may be because I didn't come up with the second solution and I refuse to admit that someone had a better solution than what I thought of (which was this one).

1.77 $\forall x \exists y \exists z(x = y^2 + z^2)$.

1.78 You may have a different answer, but here is one possibility based on the hint. If we let $P(x, y)$ be $x < y$ where the domain for both is the real numbers, then $\forall x \exists y(x < y)$ is true since for

any given x, we can choose $y = x + 1$. However, $\exists y \forall x(x < y)$ is false since no matter what value we pick for y, $x < y$ is false for $x = y + 1$. In other words, it is not true for *all* values of x. As with the previous examples, the difference is that in this case we need to have a single value of y that works for *all* values of x.

1.82

(a) It is saying that every integer can be written as two times another integer. Simplified, it is saying that every integer is even.

(b) The most direct translation of the final line of the solution is "There is some integer that cannot be written as two times another integer for any integer." A smoothed-out translation would be "There is at least one odd integer."

(c) Since 3 is odd, the statement is clearly false.

1.85 $\neg p$, q, and r.

1.89 $\neg p$, q, $p \wedge q \wedge r$, $\neg p \wedge q$, r, $\neg r \wedge p \wedge q$.

1.92 $\neg p$, $q \vee r$, $\neg q \wedge r$, $p \wedge q \wedge r$, $\neg r \wedge p \wedge q$, $(p \wedge \neg r) \vee (r \wedge q) \vee (\neg q \wedge p)$, $(p \wedge \neg r) \vee (r \wedge q) \vee (\neg q \wedge p \wedge r)$

1.95 The truth table for $p \leftrightarrow q$ is given to the right. The first row yields conjunctive clause $p \wedge q$, and the fourth row yields conjunctive clause $\neg p \wedge \neg q$. The disjunction of these is $(p \wedge q) \vee (\neg p \wedge \neg q)$. Thus, $p \leftrightarrow q = (p \wedge q) \vee (\neg p \wedge \neg q)$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

1.97 $Y = (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$.

2.4 $2d + 1$; $c + d + 1$; even

2.6 $2n$; $2o + 1$; some integers n and o; $4no + 2n = 2(2no + n)$ or $2(n(2o + 1))$. (Your steps might vary slightly, but you should end up with either $2(2no+n)$ or $2(n(2o+1))$ in the final step); $2no+1$ or $n(2o + 1)$; 'an even integer' or 'even'.

2.7 Let a and b be even integers. Then $a = 2m$ and $b = 2n$ for some integers m and n. Their product is $ab = (2m)(2n) = 2(2mn)$ which is even since $2mn$ is an integer. *Notice that we used two different letters here! You cannot assume $a = 2n$ and $b = 2n$ because then you are assuming that $a = b$ whether or not you realize it!*

2.8 Here are my comments on the proof.

- The first sentence is phrased weird–we are not letting a and b be odd *by* the definition of odd. We are *using* the definition.
- It does not state that n and q need to be integers.
- Although it is not incorrect, using n and q is just weird in this context. It is customary to use adjacent letters, like n and m, or q and r.
- Given the above problems, I would rephrase the first sentence as *'Let a and b be an odd numbers. Then $a = 2n + 1$ and $b = 2m + 1$ for some integers n and m.'*
- There is an algebra mistake. The product should be $2(2nq + q + n)$.
- If you replace $2nq + 1$ with $2nq + q + n$ (twice) in the last sentence (see the previous item) it would be a perfect finish to the proof.

2.9 Hopefully it is clear to you that the proof *can't* be correct since the sum of an even and an odd number is odd, not even. The algebra is correct. *The problem is that* $n + m + 1/2$ *is not an integer.* In order to be even, a number must be expressed in the form $2k$ ***where*** k ***is an integer***. *Any* number can be written as $2x$ if we don't require that x be an integer, so you *cannot* say that a number is even because it is of the form $2x$ unless x is an integer.

2.13 a an integer; $(3x + 2)$; $(5x - 7)$;7; 7 divides $15x^2 - 11x - 14$.

2.15 This proof is correct. Not all of the Evaluate problems have an error!

2.17 The number 2 is positive and even but is clearly not composite since it is prime. Since the statement is false the proof must be incorrect. So where is the error? It is in the final statement. Although a can be written as the product of 2 and k, what if $k = 1$ (that is, $a = 2$). In that case we have not demonstrated that a has a factor other than a or 1, so we can't be sure that it is composite.

2.18 If you didn't get, try this hint before reading the rest of the solution: Assume a is an even number other than 2 and prove that a is composite.

Let $a > 2$ be an even integer. Then $a = 2k$ for some integer k. Since $a \neq 2$, a has a factor other than a or 1. Therefore a is not prime. Therefore 2 is the only even prime number.

2.19 It was O.K. because according to the definition of prime, only positive integers can be prime. Therefore we only needed to consider positive even integers.

2.23 This one has a combination of two subtle errors. First of all, if $a|c$ and $b|c$, that does not necessarily imply that $ab|c$. For instance, $6|12$ and $4|12$, but it should be clear that $6 \cdot 4 \nmid 12$. Second, what if $a = b$? We'll see how to fix the proof in the next example.

2.25 Since n is not a perfect square, we know that $a \neq b$. Therefore $a < b$ or $b < a$. Since a and b are just labels for two factors of n, it doesn't matter which one is larger. So we can just assume a is the smaller one without any loss of generality. By definition of composite, we know that $a > 1$. Finally, it should be pretty clear that $b < n - 1$ since if $b = n - 1$, then $n = ab = a(n - 1) \geq 2(n - 1) = 2n - 2 = n + (n - 2) > n$ since $n > 4$. But clearly $n > n$ is impossible.

2.26 We assumed that $n = a^2 > 4$, so clearly $a > 2$.

2.28

1. **Experiment**. If you aren't sure what to do, don't be afraid to try things.
2. **Read Examples**. But don't just read. Make sure you *understand* them.
3. **Practice**. It makes perfect!

2.32 Only when you read *xkcd* and you don't laugh.

2.33 If you build it and they don't come, the proposition is false. This is the only case where it is false. To see this, notice that if you build it and they do come, it is true. If you don't build it, then it doesn't matter whether or not they come–it is true.

2.35 If you don't know a programming language, then you don't know Java.

2.37 true; $\neg p$; false; p; p is true; q is false (the last two can be in either order).

2.39 If you don't know Java, then you don't know a programming language.

2.40 They are *not* equivalent. Since Java is a programming language, the proposition seems obviously true. However, what if someone knows C++ but not Java? Then they know a programming language but they don't know Java. Thus, the inverse is false. Since one is true and the other is false, the proposition and its inverse are clearly not equivalent.

2.42 If you know a programming language, then you know Java.

2.43 They are *not* equivalent. Since Java is a programming language, the proposition seems obviously true. However, what if someone knows C++ but not Java? Then they know a programming language but they don't know Java. Thus, the converse is false. Since one is true and the other is false, the proposition and its converse are clearly not equivalent.

2.46 (a) The implication states that if I get to watch "The Army of Darkness" that I will be happy. However, it doesn't say that it is the only thing that will make me happy. For instance, if I get to see "Iron Man" instead, that would also make me happy. Thus, the inverse statement is false.

(b) I will use fact that $p \to q$ is true unless p is true and q is false. The implication is true unless I watch "The Army of Darkness" and I am not happy. The contrapositive is "If I am not happy, then I didn't get to watch 'The Army of Darkness.' " This is true unless I am not happy and I watched "The Army of Darkness." Since this is exactly the same cases in which the implication are true, the implication and its contrapositive are equivalent.

2.49 $\sqrt{35}$; $10\sqrt{35}$; $3481 \geq 3500$; *nonsense* or *false* or *a contradiction.*

2.50

Evaluation of Proof 1: Here are my comments on this proof:

- It is proving the wrong thing. This proves that the product of an even number and an odd number is even. But it doesn't even do that quite correctly as we will see next.
- The first sentence is phrased weird–we are not letting a be even *by* the definition of even. We are *using* the definition.
- It does not state that n and q need to be integers.
- Although it is not incorrect, using n and q is just weird. It is customary to use adjacent letters, like n and m, or q and r.
- Given the above problems, I would rephrase the first sentence as *'Let a be an even number and b be an odd number. Then $a = 2n$ and $b = 2m + 1$ for some integers n and m.'*
- There is an algebra mistake. The product should be $2(2nq + n)$.
- The last sentence is actually perfect (again, except for the fact that it isn't proving the right thing).

Evaluation of Proof 2: This proof is incorrect. It actually proves the *converse* of the statement. (We'll learn more about converse statements later.) In other words, it proves that if at least of one of a or b is even, then ab is even. This is *not* the same thing. It is a pretty good proof of the wrong thing, but it can be improved in at least 4 ways.

- It defines a and b but never really uses them. They should be used at the beginning of the algebra steps (i.e. $a \cdot b = \cdots$) to make it clear that the algebra is related to the product of these two numbers.
- It needs to state that k and x are integers.
- As above, using k and x is weird (but not wrong). It would be better to use k and l, or x and y.
- It needs a few words to bring the steps together. In particular, sentences should not generally begin with algebra.

Taking into account these things, the second part could be rephrased as follows.

Let $a = 2n$ and $b = 2m+1$, where n and m are integers. Then $ab = (2n)(2m+1) = 4nm + 2n = 2(2nm + n)$, which is even since $2nm + n$ is an integer.

Evaluation of Proof 3: This proof is correct.

2.54 $(1,2,3)$, $(1,3,2)$, $(2,1,3)$, $(2,3,1)$, $(3,1,2)$, and $(3,2,1)$.
2.56 Since it wasn't obvious how to do a direct proof of the fact, proof by contradiction seemed like the way to go. So we begin by assuming what we want to prove (that the product is even) is false. The short answer: *Because contradiction proofs generally begin by assuming the negation of what you want to prove.*
2.57 The proof gives the justification for this, but you may have to think about it for it to entirely sink in. Consider carefully the definition of S: $S = (a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n)$. Notice it adds and subtracts terms. If $S = 0$, then the amount added and subtracted must be the same. And if you think about it for a few minutes, especially in light of the justification given in the proof, you should see why. If you can't see it right away, go back to how the a_k's are defined and think a little more. If you get totally stuck, try an example with $n = 3$ or 4.
2.60 Because $a^2 = a \cdot a$, so to list the factors of a^2 you can list the factors of a twice. Thus, a^2 has twice as many factors as a, so it must be an even number.
2.63 (1) No. (2) Yes. (3) No. (4) No. (5) Statements of the form "p implies q" are false precisely when p is true and q is false. (6) No. Whether or not you are 21, you aren't breaking the rule. (7) No. If p is false, whether or not q is true or false doesn't matter–the statement is true. Let's consider the previous question–if you do not drink alcohol, you are following the rule regardless of whether or not the statement "you are 21" is true or false.
2.64 $a > b$; $\frac{a-b}{2}$; $\frac{a-b}{2}$; $b + \frac{a}{2} - \frac{b}{2} = \frac{a}{2} + \frac{b}{2}$; subtract $\frac{a}{2}$ from both sides and multiple both sides by 2; $a > b$; contradiction; $a \leq b$.
2.66 $a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c$; multiple both sides by q^2; odd; 0; $ap^2 + bpq$ is even and cq^2 is odd, so $ap^2 + bpq + cq^2$ is odd; $bpq + cq^2$ is even and ap^2 is odd, so $ap^2 + bpq + cq^2$ is odd; $ax^2 + bx + c = 0$ does not have a rational solution if a, b, and c are odd.
2.70

Evaluation of Proof 1: This is attempting to prove the *converse*, not the contrapositive. Since the converse of a statement is not equivalent to the original statement, this is not a valid proof. Further, the proof contains an algebra mistake. Finally, it uses the property that the sum of two even integers is even. Although this is true, the problem specifically asked to prove it using the definition of even/odd.

Evaluation of Proof 2: This proof starts out correctly by using the contrapositive statement and the definition of odd. Unfortunately, the writer claims that $5(\frac{6}{5}k + 1)$ is 'clearly odd.' This is not at all clear. What about this number makes it odd? Is it expressed as $2a + 1$ for some integer a? No. Even worse, there is a fraction in it, obscuring the fact that the number is even an integer.

Evaluation of Proof 3: This proof is *really close*. The only problem is that we don't know that $6k + 5$ is odd *using the definition of odd*. All the writer needed to do is take their algebra a little further to obtain $2(3k + 2) + 1$, which is odd by the definition of odd since $3k + 2$ is an integer.

2.76 Answers will vary greatly, but one proof is: 3 and 5 are prime but $3 + 5 = 8 = 2^3$ is clearly not prime.

2.79 $2s$ is a power of two that is in the closed interval.; $2^r = 2 \cdot 2^{r-1} < 2s < 2 \cdot 2^r = 2^{r+1}$, so $s < 2^r < 2s < 2^{r+1}$, and so the interval $[s, 2s]$ contains 2^r, a power of 2.

2.80 Because these statements are contrapositives of each other. In other words, they are equivalent. Therefore you can prove either form of the statement.

2.82 If x is odd, then $x = 2k + 1$ for some integer k. Then $x + 20 = 2k + 1 + 20 = 2(k + 10) + 1$, which is odd since $k + 10$ is an integer. If $x + 20$ is odd, then $x + 20 = 2k + 1$ for some integer k. Then $x = (x + 20) - 20 = 2k + 1 - 20 = 2(k - 10) + 1$, which is odd since $k - 10$ is an integer. Therefore x is odd iff $x + 20$ is odd.

2.83 If x is odd, then $x = 2k + 1$ for some integer k. Then $x + 20 = 2k + 1 + 20 = 2(k + 10) + 1$, which is odd since $k + 10$ is an integer. If x is even, then $x = 2k$ for some integer k. Then $x + 20 = 2k + 20 = 2(k + 10)$. Since $k + 10$ is an integer, then $x + 20$ is even. Therefore x is odd iff $x + 20$ is odd.

2.84 p implies q; q implies p; p implies q; $\neg p$ implies $\neg q$

2.85

Evaluation of Proof 1: For the forward direction, they didn't use the definition of odd. Otherwise, that part is fine. For the backward direction, their proof is nonsense. They *assumed* that $x = 2k + 1$ when they wrote $(2k + 1) - 4$ in the second sentence. This need to be *proven*.

Evaluation of Proof 2: For the forward direction, they didn't specify that k was an integer. Otherwise it is correct. The second part of the proof is *not* proving the converse. It is proving the forward direction a second time using a proof by contraposition. In other words, this proof just proves the forward direction twice and does not prove the backward direction.

2.87 This only proves that $4 + 6$ is even. It says nothing about the sum of any other two even numbers.

2.89 The problem is that this is actually a proof that $x + x$ is even if x is even since $x = 2a = y$ was assumed.

2.90 Notice that 4 and 6 are even, but $4 + 6 = 10$ is not divisible by 4. So clearly the statement is incorrect. Therefore, there must be something wrong with the proof. The problem is the same as in the previous example–the proof assumed $x = y$, even if that was not the intent of the writer. So what was proven was that if x is even, then $x + x$ is divisible by 4.

2.91 Since it should be clear that the result $(-1 = 1)$ is false, the proof can't possibly be correct.

2.92 No! Example 2.91 should have made it clear that this approach is flawed.

2.93 No, you should not be convinced. As we just mentioned, whether or not the equation is true, sometimes you can work both sides to get the same thing. Thus the technique of working both sides is not valid. It doesn't guarantee anything unless you already know that the equation is valid.

2.94 Since p and q are odd, we know that $p + q$ is even, and so $\dfrac{p+q}{2}$ is an integer. But $p < q$ gives $2p < p + q < 2q$ and so $p < \dfrac{p+q}{2} < q$, that is, the average of p and q lies between them. Since p and q are consecutive primes, any number between them is composite, and so divisible by at least two primes. So $p + q = 2\left(\dfrac{p+q}{2}\right)$ is divisible by the prime 2 and by at least two other primes dividing $\dfrac{p+q}{2}$.

2.95

Evaluation of Proof 1: This is not correct. It needs to be shown that x^y can be written as c/d, where c and d are integers with $d \neq 0$. Ask yourself this: Are a^y and b^y necessarily integers?

Evaluation of Proof 2: This is not correct. If $y = 3/2$, what does it mean to multiple x by itself one and a half times?

2.96 The statement is false. There are many counterexamples, but here is an easy one: Let $x = 2$ and $y = 1/2$. Then $x^y = 2^{1/2} = \sqrt{2}$, which is irrational.

2.97

Evaluation of Proof 1: This solution has two serious flaws. First, we absolutely cannot assume x is an integer. The only thing we can assume about x is that it is rational, and not every rational number is an integer. The other problem is that the writer proved the *inverse*, not the *contrapositive*. What they needed to prove was that if $1/x$ is rational, then x is rational. So in actuality, we know is that $1/x$ is rational, not x. We need to prove that x is rational based on the assumption that $1/x$ is rational.

Evaluation of Proof 2: This is not really a proof. It just takes the statement of the problem one step further. Is the writer *sure* that $1/x$ can't be expressed as an integer over an integer? Why? There are just too many details omitted.

Evaluation of Proof 3: The biggest flaw is that this is a proof of the *inverse* statement, not the *contrapositive*. So even it the rest of the proof were correct, it would be proving the wrong thing since the *inverse* and *contrapositive* are not equivalent. But the rest is not even entirely correct because the inverse statement is not quite true. If $x = 0$, then $p = 0$ as well and the statement and proof falls apart for the same reason–you can't divide by 0.

Evaluation of Proof 4: This proof is *almost correct*. It does correctly try to prove the contrapositive, and if it had done so correctly, that would imply the original statement is true. But there is one small problem: If $a = 0$ the proof would fall apart because it would divide by 0. This possibility needs to be dealt with. This is actually not too difficult to fix. We just need to add the following sentence before the last sentence: *"Since* $0 \neq 1/x$ *for any value of* x*, we know that* $a \neq 0$*."*.

Evaluation of Proof 5: This proof is correct.

2.98

Evaluation of Proof 1: As you will prove next, the statement is actually false. Therefore the proof has to be incorrect. But where did it go wrong? It turns out they they tried to prove the wrong thing. What needed to be proved was "If p is prime then $2^p - 1$ is prime." They attempted to prove the *converse* statement, which is not equivalent. We can still learn something by evaluating their proof. It turns out that the converse is actually true, and the proof has a lot of correct elements. Unfortunately, they are not put together properly. First of all, the proof seems to be a combination of a contradiction proof and a proof by contrapositive. They needed to pick one and stick with it. Second, the arrows ($\rightarrow$) are confusing. What do they mean? I think they are supposed to be read as "implies", but a few more words are needed to make the connections between these phrases. Finally, the final statement is incorrect. This does *not* prove that all numbers of the form $2^p - 1$ are prime when p is prime.

Evaluation of Proof 2: This proof is not even close. This is a case of "I wasn't sure how to prove it so I just said stuff that sounded good." You can't argue anything about the factors of $2^p - 1$ based on the factors of 2^p. Further, although $2^p - 1$ being odd means 2 is not a factor, it doesn't tell us whether or not the number might have *other* factors.

2.99 Notice that 11 is prime but that $2^{11} - 1 = 23 \cdot 89$ is not. Therefore, not all numbers of the form $2^p - 1$, where p is prime, are prime.

3.5 The prime numbers less than 10 are 2, 3, 5, and 7. But the problem asked for the *set of* prime numbers less than 10. Therefore, the answer is $\{2, 3, 5, 7\}$. If you were asked to *list* the prime numbers less than 10, an appropriate answer would have been $2, 3, 5, 7$ (but that is not what was asked). The cardinality of the set is 4. That is, $|\{2, 3, 5, 7\}| = 4$.

3.8 6; 5; 6; A and C represent the same set. That is, $A = C$.

3.11 ∞; ∞. You might think it is $\infty/2$, but you can't do arithmetic with ∞ since it isn't a number. Without getting too technical, although $\mathbb{Z}^+$ seems to have about half as many elements as $\mathbb{Z}$, it actually doesn't. It has the exact same number: ∞. ; 0.

3.14 $\{2a : a \in \mathbb{Z}\}$ and $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$.

3.17 $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}$.

3.20 (a) Yes. (b) Yes. A is a proper subset since 25, for instance, is in S but not in A. (c) Yes. Every set is a subset of itself. (d) No. No subset is a *proper subset* of itself. (e) No. $25 \in S$, but $25 \notin A$.

3.21 (a) yes. Any number that is divisible by 6 is divisible by 2.; (b) yes. Any number that is divisible by 6 is divisible by 3.; (c) no. $4 \in B$, but $4 \notin A$.; (d) no. $4 \in B$, but $4 \notin C$.; (e) no. $3 \in C$, but $3 \notin A$.; (f) no. $3 \in C$, but $3 \notin B$.

3.24 We will use the result of example 3.23. A subset of $\{a, b, c, d\}$ either contains d or it does not. Since the subsets of $\{a, b, c\}$ do not contain d, we simply list all the subsets of $\{a, b, c\}$ and then to each one of them we add d. This gives

$$\begin{array}{lcllcl}
S_1 &=& \varnothing & S_9 &=& \{d\} \\
S_2 &=& \{a\} & S_{10} &=& \{a, d\} \\
S_3 &=& \{b\} & S_{11} &=& \{b, d\} \\
S_4 &=& \{c\} & S_{12} &=& \{c, d\} \\
S_5 &=& \{a, b\} & S_{13} &=& \{a, b, d\} \\
S_6 &=& \{b, c\} & S_{14} &=& \{b, c, d\} \\
S_7 &=& \{a, c\} & S_{15} &=& \{a, c, d\} \\
S_8 &=& \{a, b, c\} & S_{16} &=& \{a, b, c, d\}
\end{array}$$

3.27 Based on the answer to Exercise 3.24, we have that $P(\{a, b, c, d\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}, \{d\}, \{a, d\}, \{b, d\}, \{c, d\}, \{a, b, d\}, \{b, c, d\}, \{a, c, d\}, \{a, b, c, d\}\}$. Notice that a list of these 16 sets not separated by commas and not enclosed in $\{\}$ is not correct. It may have the correct *content*, but it is not in the proper *form*.

3.29 (a) By Theorem 3.28, $|P(A)| = 2^4 = 16$. (b) Similarly, $|P(P(A))| = 2^{16} = 65536$. (c) This is just getting a bit ridiculous, but the answer is $|P(P(P(A)))| = 2^{65536}$.

3.30 Applying Theorem 3.28, it is not too hard to see that the power set will be twice as big after a single element is added.

3.33 $\mathbb{Z}$, or the set of (all) integers.

3.36 $\varnothing$.

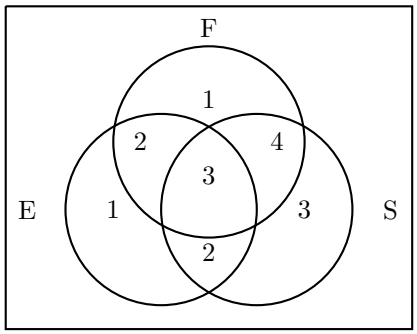
3.39 A; B.

3.43 B; A.

3.47 Since no integer is both even and odd, A and B are disjoint.

3.49 Let E be the set of all English speakers, S the set of Spanish speakers and F the set of

French speakers in our group. We fill-up the Venn diagram (to the right) successively. In the intersection of all three we put 3. In the region common to E and S which is not filled up we put $5-3=2$. In the region common to E and F which is not already filled up we put $5-3=2$. In the region common to S and F which is not already filled up, we put $7-3=4$. In the remaining part of E we put $8-2-3-2=1$, in the remaining part of S we put $12-4-3-2=3$, and in the remaining part of F we put $10-2-3-4=1$. Therefore, $1+2+3+4+1+2+3=16$ people speak at least one of these languages.



3.52 $A \times B = \{(1,3),(2,3),(3,3),(4,3)\}$.

3.55 $A^2 = \{(0,0),(0,1),(1,0),(1,1)\}$.

$A^3 = \{(0,0,0),(0,1,0),(1,0,0),(1,1,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\}$.

3.58 (a) $10*50=500$ (b) $10*20=200$ (c) $50*50*50=125,000$ (d) $10*50*20=10,000$

3.59

Evaluation of Solution 1: Although it is on the right track, this solution has several problems. First, it would be better to make it more clear that the assumption is that *both* A and B are not empty. But the bigger problem is the statement '(a,b) is in the cross product'. The problem is that a and b are not defined anywhere. Saying 'where $a \in A$ and $b \in B$' earlier does not guarantee that there is such an a or b. The proof needs to say something along the lines of 'Since A and B are not empty, then there exist some $a \in A$ and $b \in B$. Therefore $(a,b) \in A \times B \ldots$'

Evaluation of Solution 2: This one is way off. The proof is essentially saying 'Notice that $p \to q$. Therefore $q \to p$.' But these are not equivalent statements. Although it is true that if both A and B are the empty set, then $A \times B$ is also the empty set, this does not prove that both A and B must be empty in order for $A \times B$ to be empty. In fact, this isn't the correct conclusion.

Evaluation of Solution 3: The conclusion is incorrect, as is the proof. The problem is that the negation of 'both A and B are empty' is 'it is not the case that both A and B are empty' or 'at least one of A or B is not empty,' which is not the same thing as 'neither A nor B is empty.' So although the proof seems to be correct, it is not. The reason it seems almost correct is that except for this error, the rest of the proof follows proper proof techniques. Unfortunately, all it takes is one error to make a proof invalid.

Evaluation of Solution 4: This is a correct conclusion and proof.

3.63

Evaluation of Proof 1: This solution has several problems.

1. $x \in \{A-B\}$ means 'x is an element of the set containing $A-B$,' not 'x is an element of $A-B$.' What they meant was '$x \in A-B$.'
2. At the end of the first sentence, 'x is not $\in B$' mixes mathematical notation and English in a strange way. This should be either '$x \notin B$' or 'x is not in B.'

3. In the second sentence, the phrase '$x \in A$ and $\overline{B}$' is a strange mixture of math and English that is potentially ambiguous. It should be rephrased as something like '$x \in A$ and $x \in \overline{B}$' or 'x is in both A and $\overline{B}$.'
4. Finally, what has been shown here is that $A - B \subseteq A \cap \overline{B}$. This is only half of the proof. They still need to prove that $A \cap \overline{B} \subseteq A - B$.

Evaluation of Proof 2: Overall, this proof is very confusing and unclear. More specifically,

1. This is an attempt at working through what each set is by using the definitions. That would be fine except for two things. First, they were asked to give a set containment proof. Second, the wording of the proof is confusing and hard to follow. I do not come away from this with a sense that anything has been proven.
2. They are not using the terminology properly. The terms 'universe' or 'universal set' would be appropriate, but not 'universal' on its own (used twice). Similarly, what does the phrase 'all intersection part' mean? Also, a set doesn't 'return' anything. A set is just a set. It contains elements, but it doesn't 'do' anything.

Evaluation of Proof 3: This proof contains a lot of correct elements. In fact, the first half is on the right track. However, they jumped from $x \in A$ and $x \notin B$ to $x \in A \cap \overline{B}$. Between these statements they should say something like '$x \notin B$ is equivalent to $x \in \overline{B}$' since the latter statement is really needed before they can conclude that $x \in A \cap \overline{B}$. Also, it would be better if they had 'by the definition of intersection' before or after the statement $x \in A \cap \overline{B}$. Finally, it would help clarify the proof if the end was something like 'We have shown that whenever $x \in A - B$, $x \in A \cap \overline{B}$. Thus, $A - B \subseteq A \cap \overline{B}$.'

The second half of the proof starts out well, but has serious flaws. The statement 'This means that $x \in A$ and $x \notin B$' should be justified by the definitions of complement and intersection, and might even involve two steps. This is the same problem they had in the first half of the proof. More serious is the statement 'which is what we just proved in the previous statement'. What exactly does that mean? It is unclear how 'what we just proved' immediately leads us to the conclusion that $A - B = A \cap \overline{B}$. First we need to establish that $x \in A - B$ based on the previous statements (easy). Then we can say that $A \cap \overline{B} \subseteq A - B$. Finally, we can combine this with the first part of the proof to say that $A - B = A \cap \overline{B}$.

In summary, the first half is pretty good. It should at least make the connection between $x \notin B$ and $x \in \overline{B}$. The other suggestions clarify the proof a little, but the proof would be O.K. if they were omitted. The second half is another story. It doesn't really prove anything, but instead makes a vague appeal to something that was proven before. Not only is what they are referring to unclear, but how the proof of one direction is related to the proof of the other direction is also unclear.

3.65 $x \in C$; $x \in B$; definition of union; $(x \in B \wedge x \in C)$; distributive law (the logical one); $(x \in A \cap C)$; definition of intersection; definition of union.

3.78 (a) 45; (b) 8; (c) 3; (d) 6; (e) 0; (f) 7; (g) 7; (h) 7; (i) 11.

3.81 Since every integer is either even (of the form $2k$) or odd (of the form $2k+1$) we have two possibilities:

$$\begin{array}{lcll} (2k)^2 & = & 4k^2 & \equiv 0 \pmod 4, \text{or} \\ (2k+1)^2 & = & 4(k^2+k)+1 & \equiv 1 \pmod 4. \end{array}$$

Thus, n^2 has remainder 0 or 1 when divided by 4.

3.86 Observe that $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \bmod 7$ and $2^{n+2} \equiv 4 \cdot 2^n \bmod 7$. Hence $3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \mod 7$, for all natural numbers n.

3.89 $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \bmod 7$, and this cycle of three repeats. Thus $2^k - 5$ can leave only remainders $4 = (2-5) \bmod 7$, $6 = (4-5) \bmod 7$, or $3 = (1 - 5 \bmod 7)$ upon division by 7, none of which are 1.

3.93 -15; -7; 9; 13; 21. Notice that it is every 4th number along the number line, both in the positive and negative directions.

3.99 $\gcd(524, 118) = 2$ as demonstrated here:

step	a	b	r
1	524	118	52
2	118	52	14
3	52	14	10
4	14	10	4
5	10	4	2
6	4	2	0
7	2	0	0

3.102 You should have computed that $\gcd(867, 5309) = 1$ and therefore concluded that they are relatively prime.

3.105 (1) 9; (2) 10; (3) 9; (4) 10; (5) 9; (6) 9.

3.114 $f(x) = x \bmod 2$ works. The domain is $\mathbb{Z}$, and the codomain can be a variety of things. $\mathbb{Z}$, $\mathbb{N}$, and $\{0, 1\}$ are the most obvious choices. Note that we can pick any of these since the only requirement of the codomain is that the range is a subset of it. On the other hand, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$ could also all be given as the codomain, but they wouldn't make nearly as much sense.

3.118 (a) F. Consider $f(x) = \lfloor x \rfloor$ from $\mathbb{R}$ to $\mathbb{Z}$. (b) F. Consider $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$ which is not one-to-one. (c) T. See Theorem 3.117. (d) F. f maps 1 to two different values, so it isn't a function. (e) T. We previously showed it was onto, and it isn't difficult to see that it is one-to-one. (f) F. f is not onto, but it is one-to-one. (g) T. By definition of range, it is a subset of the codomain. (h) F. We have seen several counter examples to this. (i) F. If $a = 2$ and $b = 0$, the odd numbers are not in the range. (j) F. Same counterexample as the previous question. (k) T. The proof is similar to several previous proofs.

3.124 Let $y = 7x + 2$. Then $7x = y - 2$, so $x = (y-2)/7$. Thus, $f^{-1}(x) = (x-2)/7$ (or $\frac{x}{7} - \frac{2}{7}$).

3.127 $(f \circ g)(x) = f(x/2) = \lfloor x/2 \rfloor$, and $(g \circ f)(x) = g(\lfloor x \rfloor) = (\lfloor x \rfloor)/2$.

3.131 (a) F. f might not be onto–e.g. if $a = 2$ and $b = 0$. (b) F. Same reason as the previous question. (c) T. Since over the reals, f is one-to-one and onto. (d) F. There are several problems. First, x^2 may not even have an inverse depending on the domain (which was not specified). Second, even if it had an inverse, it certainly wouldn't be $1/x^2$. That's its reciprocal, not its inverse. Its inverse would be $\sqrt{x}$ (again, assuming the domain was chosen so that it is invertible). (e) F. This is only true if n is odd. (f) F. $\sqrt{2} \notin \mathbb{N}$, so not only is it not invertible, it can't even be defined on $\mathbb{N}$. (g) T. The nth root of a positive number is defined for all positive real numbers, so the function is well defined. It is not too difficult to convince yourself that the function is both one-to-one and onto when restricted to positive numbers, so it is invertible. (h) T. In both cases you get $1/x^2$. (i) F. $(f \circ g)(x) = f(x+1) = (x+1+1)^2 = (x+2)^2 = x^2 + 4x + 4$, and $(g \circ f)(x) = g((x+1)^2) = (x+1)^2 + 1 = x^2 + 2x + 2$, which are clearly not the same. (j) F. $(f \circ g)(x) = \lceil x \rceil$, and $(g \circ f)(x) = \lfloor x \rfloor$. (We'll leave it to you to see why this is the case.) (k) F. Certainly not. $f(3.5) = 3$, but $g(3) = 3$, not 3.5. (l) T. With the restricted domain, they are indeed inverses.

3.134 We never said it was *always* wrong to work both sides of an equation. If you are working on

an equation that you know to be true, there is absolutely nothing wrong with it. It is a problem only when you are starting with something you don't know to be true. In this case, we know that $2a - 3 = 2b - 3$ is true given the assumption made. Therefore, we are free to 'work both sides'.

3.135 Let $a, b \in \mathbb{R}$. If $f(a) = f(b)$, then $5a = 5b$. Dividing both sides by 5, we get $a = b$. Thus, f is one-to-one.

3.138 Notice that $f(4.5) = f(4) = 4$, so clearly f is not one-to-one. (Your proof may involve different numbers, but should be this simple.)

3.141 Notice that if $y = 2x + 1$, then $y - 1 = 2x$ and $x = (y - 1)/2$. Let $b \in \mathbb{R}$. Then $f((b-1)/2) = 2((b-1)/2) + 1 = b - 1 + 1 = b$. Thus, every $b \in \mathbb{R}$ is mapped to by f, so f is onto.

3.144 Since the floor of any number is an integer, there is no a such that $f(a) = 4.5$ (for instance). Thus, f is not onto.

3.145 (a) f **is not one-to-one.** See Example 3.137 for a proof. (b) The same proof from Example 3.137 works over the reals. But I guess it doesn't hurt to repeat it: Since $f(-1) = f(1) = 1$, f **is not one-to-one.** (c) Let $a, b \in \mathbb{N}$. If $f(a) = f(b)$, that means $a^2 = b^2$. Taking the square root of both sides, we obtain $\sqrt{a^2} = \sqrt{b^2}$, or $|a| = |b|$ (if you didn't remember that $\sqrt{x^2} = |x|$, you do now). But since $a, b \in \mathbb{N}$, $|a| = a$ and $|b| = b$. Thus, $a = b$. Thus, f **is one-to-one.**

3.146 If $f(a) = f(b)$, $3a - 5 = 3b - 5$. Subtracting 5 from both sides and then dividing both sides by 3, we get $a = b$. Thus, f is one-to-one. If $b \in \mathbb{R}$, notice that $f((b+5)/3) = 3((b+5)/3) - 5 = b + 5 - 5 = b$, so there is some value that maps to b. Therefore, f is onto. Since f is one-to-one and onto, it has an inverse. To find the inverse, we let $y = 3x - 5$. Then $3x = y + 5$, so $x = (y + 5)/3$. Thus, $f^{-1}(x) = (x + 5)/3$ (or $\frac{x}{3} + \frac{5}{3}$).

3.147 (a) Notice that if $f(a) = f(b)$, then $a - 7 = b - 7$ so $a = b$. Thus, f is one-to-one. Also notice that for any $b \in \mathbb{Z}$, $f(b + 7) = b + 7 - 7 = b$, so f is onto. (b) Since $g(1) = g(-1) = 1$, g is not one-to-one. Also notice that there is no integer a such that $g(a) = a^4 = 5$, so g is not onto. (c) If $h(a) = h(b)$, then $3a = 3b$ so $a = b$. Thus, h is one-to-one. But there is no integer a such that $h(a) = 3a = 1$, so a is not onto. (d) Notice that $r(0) = \lfloor 0/2 \rfloor = \lfloor 0 \rfloor = 0$ and $r(1) = \lfloor 1/2 \rfloor = \lfloor 0 \rfloor = 0$, so r is not one-to-one. But for any integer b, $r(2b) = \lfloor 2b/2 \rfloor = \lfloor b \rfloor = b$, so r is onto.

3.154 The following three cases probably make the most sense: When $a = b$, when $a < b$ and when $a > b$. These make sense because these are likely different cases in the code. Mathematically, we can think of it as follows. The possible inputs are from the set $\mathbb{Z} \times \mathbb{Z}$. The partition we have in mind is $A = \{(a, a) : a \in \mathbb{Z}\}$, $B = \{(a, b) : a, b \in \mathbb{Z}, a < b\}$, and $C = \{(a, b) : a, b \in \mathbb{Z}, a > b\}$. Convince yourself that these sets form a partition of $\mathbb{Z} \times \mathbb{Z}$. That is, they are all disjoint from each other and $\mathbb{Z} \times \mathbb{Z} = A \cup B \cup C$.

Alternatively, you might have thought in terms of a and/or b being positive, negative, or 0. Although that may make some sense, given that we are comparing a and b with each other, it probably doesn't matter exactly what values a and b have (i.e. whether they are positive, negative, or 0), but what values they have *relative to each other*. That is why the first answer is much better. With that being said, it wouldn't hurt to include several tests for each of our three cases that involve various combinations of positive, negative, and zero values.

3.155 Did you define two or more subsets of $\mathbb{Z}$? Are they all non-empty? Do none of them intersect with each other? If you take the union of all of them, do you get $\mathbb{Z}$? If so, your answer is correct! If not, try again.

3.157 Since $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ and $\mathbb{Q} \cap \mathbb{I} = \varnothing$, $\{\mathbb{Q}, \mathbb{I}\}$ is a partition of $\mathbb{R}$. Hopefully this comes as no surprise.

3.162 R is a subset of $\mathbb{Z} \times \mathbb{Z}$, so it is a relation. By the way, this relation should look familiar. Did you read the solution to Exercise 3.154?

3.163 Is it a subset of $\mathbb{Z}^+ \times \mathbb{Z}^+$? It is. So it is a relation on $\mathbb{Z}^+$.

3.165 (a) T is **not** reflexive since you cannot be taller than yourself. (b) N is reflexive because everybody's name starts with the same letter as their name does. (c) C is reflexive because everybody have been to the same city as they have been in. (d) K is **not** reflexive because you know who you are, so it is not the case that you don't know who you are. That is, $(a, a) \notin K$ for any a. (e) R is **not** reflexive because (Donald Knuth, Donald Knuth) (for instance) is not in the relation.
3.167 (a) T is **not** symmetric since if a is taller than b, b is clearly not taller than a. (b) N is symmetric since if a's name starts with the same letter as b's name, clearly b's name starts with the same letter as a's name. (c) C is symmetric since it is worded such that it doesn't distinguish between the first and second item in the pair. In other words, if a and b have been to the same city, then b and a have been to the same city. (d) K is **not** symmetric since (David Letterman, Chuck Cusack) $\in K$, but (Chuck Cusack, David Letterman) $\notin K$. (e) R is not symmetric since (Barack Obama, George W. Bush) $\in R$, but (George W. Bush, Barack Obama)$\notin R$.
3.169 (a) Just knowing that $(1, 1) \in R$ is not enough to tell either way. (b) On the other hand, if $(1, 2)$ and $(2, 1)$ are both in R, it is clearly **not** anti-symmetric.
3.170 This is just the contrapositive of the original definition.
3.171 (a) T is anti-symmetric since whenever $a \neq b$, if a is taller than b, then b is not taller than a, so if $(a, b) \in T$, then $(b, a) \notin T$. (b) N is **not** anti-symmetric since (Bono, Boy George) and (Boy George, Bono) are both in N. (c) C is **not** anti-symmetric since (Bono, The Edge) and (The Edge, Bono) are both in C (since they have played many concerts together, they have certainly been in the same city at least once). (d) Since both (Dirk Benedict, Jon Blake Cusack 2.0) and (Jon Blake Cusack 2.0, Dirk Benedict) are in K, K is **not** anti-symmetric. (e) R is anti-symmetric since it only contains one element, (Barack Obama, George W. Bush), and (George W. Bush, Barack Obama)$\notin R$.
3.172 (a) No. The relation $R = \{(1, 2), (2, 1), (1, 3)\}$ is neither symmetric ($(3, 1) \notin R$) nor anti-symmetric ($(1, 2)$ and $(2, 1)$ are both in R). (b) No. For example, R from answer (a) is not anti-symmetric, but isn't symmetric either. (c) Yes. If you answered incorrectly, don't worry. You get to think about why the answer is 'yes' in the next exercise.
3.173 Many answers will work, but they all have the same thing in common: They only contain 'diagonal' elements (but not necessarily all of the diagonal elements). For instance, let $R = \{(a, a) : a \in \mathbb{Z}\}$. Go back to the definitions for symmetric and anti-symmetric and verify that this is indeed both. Another examples is $R = \{(\text{Ken}, \text{Ken})\}$ on the set of English words.
3.175 (a) T is transitive since if a is taller than b, and b is taller than c, clearly a is taller than c. In other words $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$. (b) N is transitive because if a's name starts with the same letter as b's name, and b's name starts with the same letter as c's name, clearly it is the same letter in all of them, so a's name starts with the same letter as c's. (c) C is **not** transitive. You might think a similar argument as in (a) and (b) works here, but it doesn't. The proof from (b) works because names start with a single letter, so transitivity holds. But if $(a, b) \in C$ and $(b, c) \in C$, it might be because a and b have both been to Chicago, and b and c have both been to New York, but that a has never been to New York. In this case, $(a, c) \notin C$. So C is not transitive. (d) K is not transitive. For instance, (David Letterman, Chuck Cusack) $\in K$ and (Chuck Cusack, David Letterman's son) $\in K$, but (David Letterman, David Letterman's son) $\notin K$ since I sure hope he knows his own son. (e) R is transitive since there isn't even an $a, b, c \in R$ such that (a, b) and (b, c) are both in R, so it holds vacuously.
3.178 (a) T is **not** an equivalence relation since it is not symmetric. (b) N is an equivalence relation since it is reflexive, symmetric, and transitive. (c) C is **not** an equivalence relation since it is not transitive. (d) K is **not** an equivalence relation since it is not reflexive, symmetric, or transitive. This one isn't even close! (e) R is **not** an equivalence relation since it is not reflexive.

3.180 (a) T is a **not** partial order because it is not reflexive. (b) N is **not** a partial order since it is not anti-symmetric. (c) C is **not** a partial order since it is not anti-symmetric or transitive. (d) K is **not** a partial order since it is not reflexive, anti-symmetric, or transitive. (e) R is **not** a partial order since it is not reflexive.

3.181 In the following, A, B, and C are elements of X. As such, they are sets.

(**Reflexive**) Since $A \subseteq A$, $(A, A) \in R$, so R is reflexive.

(**Anti-symmetric**) If $(A, B) \in R$ and $(B, A) \in R$, then we know that $A \subseteq B$ and $B \subseteq A$. By Theorem 3.60, this implies that $A = B$. Therefore R is anti-symmetric.

(**Transitive**) If $(A, B) \in R$ and $(B, C) \in R$, then $A \subseteq B$ and $B \subseteq C$. But the definition of $\subseteq$ implies that $A \subseteq C$, so $(A, C) \in R$, and R is transitive.

Since R is reflexive, anti-symmetric, and transitive, it is a partial order.

3.182 (a) Since $(1, 1) \notin R$, R is not reflexive. (b) Since $(1, 2) \in R$, but $(2, 1) \notin R$, R is not symmetric. (c) A careful examination of the elements reveals that it *is* anti-symmetric. (d) A careful examination of the elements reveals that it *is* transitive. (e) Since it is not reflexive or symmetric, it is not an equivalence relation. (f) Since it is not reflexive, it is not a partial order.

3.184 $((a, b), (a, b))$; bc; da; $((c, d), (a, b))$; symmetric; $ad = bc$; $cf = de$; de/f; $b(de/f)$; $af = be$; $((a, b), (e, f))$

4.3 (a)$x_0 = 1 + (-2)^0 = 1 + 1 = 2$ (b)$x_1 = 1 + (-2)^1 = 1 - 2 = -1$ (c)$x_2 = 1 + (-2)^2 = 1 + 4 = 5$ (d)$x_3 = 1 + (-2)^3 = 1 - 8 = -7$ (e)$x_4 = 1 + (-2)^4 = 1 + 16 = 17$

4.4 We will just provide the final answer for these. If you can't get these answers, you may need to brush up on your algebra skills. (a) 2, 1/2,5/4, 7/8, 17/16; (b) 2, 2, 3, 7, 25; (c) 1/3, 1/5, 1/25, 1/119, 1/721; (d) 2, 9/4, 64/27, 625/256, 7776/3125

4.8 Notice that $x_0 = 1$, $x_1 = 5 \cdot 1 = 5$, $x_2 = 5 \cdot 5 = 5^2$, $x_3 = 5 \cdot 5^2 = 5^3$, etc. Looking back, we can see that $1 = 5^0$, so $x_0 = 5^0$. Also, $x_1 = 5 = 5^1$. So it seems likely that the solution is $x_n = 5^n$. This is *not* a proof, though!

4.9 Notice that $x_0 = 1$, $x_1 = 1 \cdot 1 = 1$, $x_2 = 2 \cdot 1 = 2$, $x_3 = 3 \cdot 2 = 6$, $x_4 = 4 \cdot 6 = 24$, $x_3 = 5 \cdot 24 = 120$, etc. Written this way, no obvious pattern is emerging. Sometimes *how* you write the numbers matters. Let's try this again: $x_1 = 1 \cdot 1 = 1!$, $x_2 = 2 \cdot 1 = 2!$, $x_3 = 3 \cdot 2 \cdot 1 = 3!$, $x_4 = 4 \cdot 3 \cdot 2 \cdot 1 = 4!$, $x_3 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5!$, etc. Now we can see that $x_n = n!$ is a likely solution. Again, this isn't a proof.

4.10 Their calculations are correct (Did you check them with a calculator? You *should* have! How else can you tell whether or not their solution is correct?). So it does seem like $a_n = 2^n$ is the correct solution. However,

$$a_5 = \left\lfloor \tfrac{1+\sqrt{5}}{2} \times a_4 \right\rfloor + a_3 = \left\lfloor \tfrac{1+\sqrt{5}}{2} \times 16 \right\rfloor + 8 = 33 \neq 2^5$$

so the solution that seems 'obvious' turns out to incorrect. We won't give the actual solution since the point of this example is to demonstrate that just because a pattern holds for the first several terms of a sequence, it does not guarantee that it holds for the whole sequence.

4.12 Hopefully you came up with the solution $x_n = 5^n$. Since $x_0 = 1 = 5^0$, it works for the initial condition. If we plug this back into the right hand side of $x_n = 5 \cdot x_{n-1}$, we get

$$\begin{aligned} 5 \cdot x_{n-1} &= 5 \cdot 5^{n-1} \\ &= 5^n \\ &= x_n, \end{aligned}$$

which verifies the formula. Therefore $x_n = 5^n$ is the solution.

4.13 Hopefully you came up with the solution $x_n = n!$. Since $x_0 = 1 = 0!$, it works for the initial condition. If we plug this back into the right hand side of $x_n = n \cdot x_{n-1}$, we get

$$\begin{aligned} n \cdot x_{n-1} &= n \cdot (n-1)! \\ &= n! \\ &= x_n, \end{aligned}$$

which verifies the formula. Therefore $x_n = n!$ is the solution.

4.14 The computations are correct, the conclusion is correct, but unfortunately, the final code has a serious problem. It works *most* of the time, but it does not deal with negative values correctly. It should return 3 for all negative values, but it continues to use the formula. The problem is they forgot to even consider what the function does for negative values of n. They probably could have formatted their answer better, too. It's difficult to follow in paragraph form. They could have put the various values of `ferzle(n)` each on their own line and presented it mathematically instead of in sentence form. For instance, instead of 'ferzle(1) returns ferzle(0)+2, which is $3 + 2 = 5$,' they should have '$ferzle(1) = ferzle(0) + 2 = 3 + 2 = 5$.' It would have made it much easier to see the pattern.

4.15

```
int ferzle(int n) {
        if(n<=0) {
            return 3;
    } else {
            return 2*n+3;
        }
}
```

4.19 We didn't do anything wrong. We wrote the inequality in the other order, and the indexes are one lower than those given in the definition. But that's O.K. The definition is simply trying to convey the idea that every term is strictly greater than the previous. That is what we showed. We can show that $x_n < x_{n+1}$, $x_{n+1} > x_n$, $x_{n-1} < x_n$, or $x_n > x_{n-1}$. They all mean essentially the same thing. The only difference is the order in which the inequalities are written (the first two and last two are saying exactly the same thing–we just flipped the inequality) and what values of n are valid. For instance, if the sequence starts at 0, then we need to assume $n \geq 0$ for the first pair of inequalities and $n \geq 1$ for the second pair.

4.21 If you got stuck on this one, first realize that $x_n = \dfrac{n^2+1}{n} = n + \dfrac{1}{n}$. This form might make the algebra a little easier. Then, follow the technique of the previous example–show that $x_{n+1} - x_n > 0$. So, if necessary, go back and try again. If you already attempted a proof, you may proceed to read the solution.

Notice that,

$$\begin{aligned} x_{n+1} - x_n &= \left(n + 1 + \frac{1}{n+1}\right) - \left(n + \frac{1}{n}\right) \\ &= 1 + \frac{1}{n+1} - \frac{1}{n} \\ &= 1 - \frac{1}{n(n+1)} \\ &> 0, \end{aligned}$$

the last step since $1/n(n+1) < 1$ when $n \geq 1$. Therefore, $x_{n+1} - x_n > 0$, so $x_{n+1} > x_n$, i.e., the sequence is strictly increasing. If your solution is significantly different than this, make sure you determine one way or another if it is correct.

4.22 We could go into much more detail than we do here, and hopefully you did when you wrote down your solutions. But we'll settle for short, informal arguments this time. (a) This is just a linear function. It is **strictly increasing**. (b) Since this keeps going from positive to negative to positive, etc. it is **non-monotonic**. (c) We know that $n!$ is strictly increasing. Since this is the reciprocal of that function, it is almost *strictly decreasing* (since we are dividing by a number that is getting larger). However, since $1/0! = 1/1! = 1$, it is just **decreasing**. (d) This is getting closer to 1 as n increases. It is **strictly increasing** (e) This is $n(n-1)$. $x_1 = 0$, $x_2 = 2$, $x_3 = 6$, etc. Each term is multiplying two numbers that are both getting larger, so it is **strictly increasing**. (f) This is similar to the previous one, but $x_0 = x_1 = 0$, so it is just **increasing**. (g) This alternates between -1 and 1, so it is **non-monotonic**. (h) Each term subtracts from 1 a smaller numbers than the last term, so it is **strictly increasing**. (i) Each term adds to 1 a smaller number than the last term, so it is **strictly decreasing**.

4.26 You should have concluded that $a = -\frac{2}{3^{17}}$ and that $r = \frac{2}{3^{16}} / \left(-\frac{2}{3^{17}}\right) = -3^{17}/3^{16} = -3$ (or you could have divided the second and third terms). Then the n-th term is $-\frac{2}{3^{17}}(-3)^{n-1} = \frac{2(-1)^n}{3^{18-n}}$ (Make sure you can do the algebra to get to this simplified form). Finally, the 17th term is $\frac{2(-1)^{17}}{3^{18-17}} = -\frac{2}{3}$

4.28 We are given that $ar^5 = 20$ and $ar^9 = 320$. Dividing, we can see that $r^4 = 16$. Thus $r = \pm 2$. (We don't have enough information to know which it is). Since $ar^5 = 20$, we know that $a = 20/r^5 = \pm 20/32$. So the third term is $ar^2 = (\pm 20/32)(\pm 2)^2 = \pm 80/32 = \pm 5/2$. Thus $|ar^2| = 5/2$.

4.32

(a) The difference between the each of the first 4 terms of the sequence is 7, so it appears to be an arithmetic sequence. Doing a little math, the correct answer appears to be (d) 51.

(b) Although the sequence *appears to be* arithmetic, we cannot be certain that it is. If you are told it is arithmetic, then 51 is absolutely the correct answer. Notice that the previous example specifically stated that you should assume that the pattern continues. This one did not. Without being told this, the rest of the sequence could be anything. The 8th term could be 0 or $8,675,309$ for all we know. Of the choices given, 51 is the most *obvious* choice, but any of the answers could be correct. This is one reason I hate these sorts of questions on tests.

Although I think it is important to point out the flaw in these sorts of questions, it is also important to conform to the expectations when answering such questions on standardized tests. In other words, instead of disputing the question (as some students might be inclined to do), just go with the obvious interpretation.

4.33 (a) The closed form was $x_n = 5^n$, which is clearly geometric (with $a = 1$ and $r = 5$) and not arithmetic. (b) Since the solution for this one is $x_n = n!$, this is neither arithmetic or geometric. (c) Since the sequence is essentially $f_n = 2n + 3$, with initial condition $f_0 = 3$, it is an arithmetic sequence. It is clearly not geometric.

4.36 $\displaystyle\sum_{i=0}^{100} y^i$

4.38 $\displaystyle\sum_{i=0}^{50} (y^2)^i$ or $\displaystyle\sum_{i=0}^{50} y^{2i}$

4.40 (a) 2 (b)11 (c) 100 (d) 101

4.45 (a) $\displaystyle\sum_{k=5}^{6} 5 = 5\sum_{k=5}^{6} 1 = 5 \cdot 2 = 10$. (b) $\displaystyle\sum_{k=20}^{30} 200 = 200\sum_{k=20}^{30} 1 = 200(30 - 20 + 1) = 2200$.

4.48 Using Theorem 4.46, we get the following answers: (a) $(30-20+1)200 = 11*200 = 2200$. (b) 900 (c) 909. Notice that this one has one more term than the previous one. The fact that the additional index is 0 doesn't matter since it is adding 9 for that term.

4.49 This solution contains an 'off by one' error. The correct answer is $10(75-25+1) = 10*51 = 510$.

4.52 (a) $20 \cdot 21/2 = 210$ (b) $100 \cdot 101/2 = 5050$ (c) $1000 \cdot 1001/2 = 500500$

4.53

Evaluation of Solution 1: Another example of the 'off by one error'. They are using the formula $n(n-1)/2$ instead of $n(n+1)/2$.

Evaluation of Solution 2: This answer doesn't even make sense. What is k in the answer? k is just an index of the summation. The index should *never* appear in the answer. The problem is that you can't pull the k out of the sum since each term in the sum depends on it.

4.54 It is true. The additional term that the sum adds is 0, so the sum is the same whether or not it starts at 0 or 1.

4.57 $$\sum_{i=1}^{100} 2 - i = \sum_{i=1}^{100} 2 - \sum_{i=1}^{100} i = 200 - \frac{100 \cdot 101}{2} = 200 - 5050 = -4850.$$

4.58 The sum of the first n odd integers is

$$\sum_{k=1}^{n}(2k-1) = \sum_{k=1}^{n} 2k - \sum_{k=1}^{n} 1 = 2\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 = 2\frac{n(n+1)}{2} - n = n^2 + n - n = n^2.$$

4.61 (a) $$\sum_{k=10}^{20} k = \sum_{k=1}^{20} k - \sum_{k=1}^{9} k = 20 \cdot 21/2 - 9 \cdot 10/2 = 210 - 45 = 165.$$

(b) $$\sum_{k=21}^{40} k = \sum_{k=1}^{40} k - \sum_{k=1}^{20} k = 40 \cdot 41/2 - 20 \cdot 21/2 = 820 - 210 = 610.$$

4.62

Evaluation of Solution 1: Another example of the off-by-one error. The second sum should end at 29, not 30.

Evaluation of Solution 2: This one has two errors, one of which is repeated twice. It has the same error as the previous solution, but it also uses the incorrect formula for each of the sums (the off-by-one error).

Evaluation of Solution 3: This one is correct.

4.63 Two errors are made that cancel each other out. The first error is that the second sum in the second step should go to 29, not 30. But in the computation of that sum in the next step, the formula $n(n-1)/2$ is used instead of $n(n+1)/2$ (The correct formula was used for the first sum). This is a rare case where an off-by-one error is followed by the opposite off-by-one error that results in the correct answer.

It should be emphasized that even though the correct answer is obtained, *this is an incorrect solution.* They obtained the correct answer by sheer luck.

4.65 There are two ways to answer this. The smart aleck answer is 'because it is correct.' But *why* is it correct with 2, and couldn't it be slightly modified to work with 1 or 0? The answer is *no* because if you plug 1 or 0 into $\frac{1}{(k-1)k}$, you get a division by 0. Hopefully I don't need to tell you that this is a bad thing.

4.66

$$\begin{aligned}\sum_{k=1}^{n} k^3 + k &= \sum_{k=1}^{n} k^3 + \sum_{k=1}^{n} k \\ &= \frac{n^2(n+1)^2}{4} + \frac{n(n+1)}{2} \\ &= \frac{n(n+1)}{2}\left(\frac{n(n+1)}{2} + 1\right) \\ &= \frac{n(n+1)}{2}\left(\frac{n^2+n+2}{2}\right) \\ &= \frac{n(n+1)(n^2+n+2)}{4}\end{aligned}$$

4.68 (a) $\sum_{i=1}^{n}\sum_{j=1}^{i} 1 = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

(b) $\sum_{i=1}^{n}\sum_{j=1}^{i} j = \sum_{i=1}^{n} \frac{i(i+1)}{2} = \cdots = \frac{n(n+1)(n+2)}{6}$. (This one involves doing a little algebra, applying two formulas, and then doing a little more algebra. Make sure you work it out until you get this answer.)

(c) $\sum_{i=1}^{n}\sum_{j=1}^{n} ij = \sum_{i=1}^{n}\left(i\sum_{j=1}^{n} j\right) = \sum_{i=1}^{n}\left(i\frac{n(n+1)}{2}\right) = \frac{n(n+1)}{2}\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\frac{n(n+1)}{2} = \frac{n^2(n+1)^2}{4}$.

4.72 $\frac{3^{50}-1}{2} = 358948993845926294385124$.

4.73 This is equivalent to $\sum_{k=0}^{34}(-2)^k$, so the summation is $(1-(-2)^{35})/(1-(-2)) = (1-(-1)^{35}2^{35})/3 = (1+2^{35})/3 = 11453246123$.

4.74 (a) $\frac{1-y^{101}}{1-y}$ or $\frac{y^{101}-1}{y-1}$ (We won't give the alternatives for the rest. If your answer differs, do some algebra to make sure it is equivalent.) (b) $\frac{1-(-y)^{101}}{1-(-y)} = \frac{1+y^{101}}{1+y}$ (c) $\frac{1-y^{102}}{1-y^2}$.

4.77 $x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$.

4.78 $2^1 + 2^2 + 2^3 + \cdots + 2^{n+1}$; 2^0; 2^{n+1}; $2^{n+1} - 2^0$

4.80 $a\sum_{k=0}^{n} r^k$; $a\frac{1-r^{k+1}}{1-r}$.

4.81 Let $S = a + ar + ar^2 + \cdots + ar^n$. Then $rS = ar + ar^2 + \cdots + ar^{n+1}Z$, so

$$\begin{aligned}S - rS &= a + ar + ar^2 + \cdots + ar^n - ar - ar^2 - \cdots - ar^{n+1} \\ &= a - ar^{n+1}.\end{aligned}$$

From this we deduce that

$$S = \frac{a - ar^{n+1}}{1-r},$$

that is,

$$\sum_{k=0}^{n} ar^k = \frac{a - ar^{n+1}}{1-r}.$$

4.92 $A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix}$

4.96 $\mathbf{0}_{3\times 4} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $\mathbf{I}_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

4.99 $A + 2B = \begin{bmatrix} -1 & 3 \\ 3 & 3 \\ 0 & 0 \end{bmatrix}$

4.100 $M + N = \begin{bmatrix} a+1 & 0 & 2c \\ a & b-2a & 0 \\ 2a & 0 & -2 \end{bmatrix}$, $2M = \begin{bmatrix} 2a & -4a & 2c \\ 0 & -2a & 2b \\ 2a+2b & 0 & -2 \end{bmatrix}$

4.102 $x = 1$ and $y = 4$.

4.105 $AA = \begin{bmatrix} 2 & 1 & 3 \\ 0 & 1 & 1 \\ 4 & 4 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 3 \\ 0 & 1 & 1 \\ 4 & 4 & 0 \end{bmatrix} = \begin{bmatrix} 16 & 15 & 7 \\ 4 & 5 & 1 \\ 8 & 8 & 16 \end{bmatrix}$

4.107 $AB = \begin{bmatrix} a & b & c \\ c+a & a+b & b+c \\ a+b+c & a+b+c & a+b+c \end{bmatrix}$, $BA = \begin{bmatrix} a+b+c & b+c & c \\ a+b+c & a+b & b \\ a+b+c & c+a & a \end{bmatrix}$

4.110 $\begin{bmatrix} 32 & -32 \\ -32 & 32 \end{bmatrix}$.

4.115 Observe that $A^2 = (AB)(AB) = A(BA)B = A(B)B = (AB)B = AB = A$. Similarly, $B^2 = (BA)(BA) = B(AB)A = B(A)A = (BA)A = BA = B$.

4.116 Disprove! Take $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then $AB = B$, but $BA = \mathbf{0}_2$.

4.120 We have $\operatorname{tr}\left(A^2\right) = \operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \operatorname{tr}\left(\begin{bmatrix} a^2+bc & ab+bd \\ ca+cd & d^2+cb \end{bmatrix}\right) = a^2 + d^2 + 2bc$ and $\left(\operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\right)^2 = (a+d)^2$. Thus $\operatorname{tr}\left(A^2\right) = (\operatorname{tr}(A))^2 \iff a^2 + d^2 + 2bc = (a+d)^2 \iff bc = ad$, is the condition sought.

4.123 $N^T = \begin{bmatrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{bmatrix}$.

4.127 We have $(AB - BA)^T = (AB)^T - (BA)^T = B^T A^T - A^T B^T = -BA - A(-B) = AB - BA$.

5.6 (a) Since we assumed that $n \geq 1$, $-3n$ is certainly negative. In other words, $-3n \leq 0$. That's why in the first step we could say that $5n^2 - 3n + 20 \leq 5n^2 + 20$. (b) We used the fact that $20 \leq 20n^2$ whenever $n \geq 1$. If either of these solutions is not clear to you, you need to brush up on your algebra.

5.7 This is incorrect. It is *not true* that $-12n \leq -12n^2$ when $n \geq 1$. (If this isn't clear to you after thinking about it for a few minutes, you may need to do some algebra review.) In fact, that error led to the statement $4n^2 - 12n + 10 \leq 2n^2$ which cannot possibly be true as n gets larger since it would require that $2n^2 - 12n + 10 \leq 0$. This is not true as n gets larger. In fact, when $n = 10$, for instance, it is clearly not true. But it *is true* that $-12n < 0$ when $n \geq 0$, so instead of replacing it with $-12n^2$, it should be replaced with 0 as in previous examples.

5.8 (a) Sure. Add the final step of $25n^2 \leq 50n^2$ to the algebra in the proof. In fact, any number above 25 can easily be used. Some values under 25 can also be used, but they would require a modification of the algebra used in the proof. The bottom line is that there is generally no 'right' value to use for c. If you find a value that works, then it's fine. (b) Clearly not. For this to work, we would need $5n^2 - 3n + 20 < 2n^2$ to hold as n increases towards ∞. But this would imply that $3n^2 - 3n + 20 < 0$. But when $n \geq 1$, $3n^2$ is positive and larger than $3n$, so $3n^2 - 3n + 20 > 0$. (c) Sure. The proof used the fact that the inequality is true when $n \geq 1$, so it is clearly also true if $n \geq 100$. And the definition of Big-O does not require that we use the smallest possible value for n_0. (d) No. We would need a constant c such that $5 \cdot 0^2 - 3 \cdot 0 + 20 = 20 \leq 0 = c \cdot 0^2$, which is clearly impossible.

5.9 If $n \geq 1$,

$$\begin{aligned} 5n^5 - 4n^4 + 3n^3 - 2n^2 + n &\leq 5n^5 + 3n^3 + n \\ &\leq 5n^5 + 3n^5 + n^5 \\ &= 9n^5. \end{aligned}$$

Therefore, $5n^5 - 4n^4 + 3n^3 - 2n^2 + n = O(n^5)$.

5.10 We used $n_0 = 1$ and $c = 9$. Your values for n_0 and c may differ. This is O.K. if you have the correct algebra to back it up.

5.13 Since $4n^2 \leq 4n^2 + n + 1$ for $n \geq 0$, $4n^2 = \Omega(n^2)$.

5.14 We used $c = 4$ and $n_0 = 0$. You might have used $n_0 = 1$ or some other positive value. As long as you chose a positive value for n_0, it works just fine. You could have also used any value for c larger than 0 and at most 4.

5.17 It is O.K. Since the second inequality holds when $n \geq 0$, it also holds when $n \geq 1$.

In general, when you want to combine inequalities that contain two different assumptions, you simply make the more restrictive assumption. In this case, $n \geq 1$ is more restrictive than $n \geq 0$. In general, if you have assumptions $n \geq a$ and $n \geq b$, then to combine the results with these assumptions, you assume $n \geq max(a, b)$.

5.22 $g(n)$ appears in the denominator of a fraction. If at some point it does not become (and remain) non-zero, the limit in the definition will be undefined. If you never took a calculus course and are not that familiar with limits, do not worry a whole lot about this subtle point.

5.23 o is like $<$ and ω is like $>$.

5.24 (a) No. If $f(n) = \Theta(g(n))$, f and g grow at the same rate. But $f(n) = o(g(n))$ expresses the idea that f grows slower than g. It is impossible for f to grow at the same rate as g and slower than g. (b) Yes! If f grows no faster than g, then it is possible that it grows slower. For instance, $n = O(n^2)$ and $n = o(n^2)$ are both true. (c) No. If f and g grow at the same rate, then $f(n) = O(g(n))$, but $f(n) \neq o(g(n))$. For instance, $3n = O(n)$, but $3n \neq o(n)$. (d) Yes. In fact, it is guaranteed! If f grows slower than g, then f grows no faster than g.

5.25

Evaluation of Solution 1: Although this proof sounds somewhat reasonable, it is way too informal and convoluted. Here are some of the problems.

1. This student misunderstands the concept behind 'ignoring the constants.' We can ignore the constants *after we know that* $f(n) = O(g(n))$. We can't ignore them in order to prove it.
2. The phrase 'become irrelevant' (used twice) is not precise. We have developed mathematical notation for a reason—it allows us to make statements like these precise. It's

kind of like saying that a certain car costs 'a lot'. What is 'a lot'? Although \$30,000 might be a lot for most of us, people with a lot more money than I have might not think that \$500,000 is a lot.

3. The phrase 'This leaves us with $n^k + n^{k-1} + \cdots + n = O(n^k)$' is odd. What precisely do they mean? That this is true or that this is what we need to prove now? In either case, it is incorrect. Similarly for the second time they use the phrase 'This leaves us with'.
4. The second half of the proof is unnecessarily convoluted. They essentially are claiming that their proof has boiled down to showing that $n^k = O(n^k)$. To prove this, they use an incredibly drawn out, yet vague, explanation that is in a single unnecessarily long sentence. Why are they even bringing Θ and Ω into this proof? Why don't they just say something like 'since $n^k \leq 1n^k$ for all $n \geq 1$, $n^k = O(n^k)$'? I believe the answer is obvious: they don't really understand what they are doing here. They clearly have a vague understanding of the notation, but they don't understand the formal definition.

The bottom line is that this student understands that the statement they needed to prove is correct, and they have a vague sense of *why* it is true, but they did not have a clear understanding of how to use the definition of Big-O to prove it. The most important thing to take away from this example is this: *Be precise, use the notation and definitions you have learned, and if your proofs look a lot different than those in the book, you might question whether or not you are on the right track.*

Evaluation of Solution 2: This proof is correct.

5.26 We cannot say anything about the relative growth rates of $f(n)$ and $g(n)$ because we are only given upper bounds for each. It is possible that $f(n) = n^2$ and $g(n) = n$, so that $f(n)$ grows faster, or vice-versa. They could also both be n.
5.27 (a) F. This is saying that $f(n)$ grows *no* faster than $g(n)$. (b) F. They grow at the same rate. (c) F. $f(n)$ might grow slower than $g(n)$. For instance, $f(n) = n$ and $g(n) = n^2$. (d) F. They might grow at the same rate. For instance, $f(n) = g(n) = n$. (e) F. If $f(n) = n$ and $g(n) = n^2$, $f(n) = O(g(n))$, but $f(n) \neq \Omega(g(n))$. (f) T. By Theorem 5.18. (g) F. If $f(n) = n$ and $g(n) = n^2$, $f(n) = O(g(n))$, but $f(n) \neq \Theta(g(n))$. (h) F. If $f(n) = n$ and $g(n) = n^2$, $f(n) = O(g(n))$, but $g(n) \neq O(f(n))$.
5.37 $c_1 g(n) \leq f(n) \leq c_2 g(n)$ for all $n \geq n_0$; $\frac{1}{c_2} f(n)$; $\frac{1}{c_1} f(n)$; $c_3 h(n) \leq g(n) \leq c_4 h(n)$ for all $n \geq n_1$.; c_2; $c_2 c_4$; $\max\{n_0, n_1\}$; $c_1 c_3 h(n)$; $c_2 c_4 h(n)$; $\Theta(h(n))$; Θ; transitive;
5.39 (a) T. By Theorem 5.36. (b) T. By Theorem 5.18. (c) T. By Theorem 5.32. (d) F. The backwards implication is true, but the forward one is not. For instance, if $f(n) = n$ and $g(n) = n^2$, clearly $f(n) = O(g(n))$, but $f(n) \neq \Theta(g(n))$. (e) F. Neither direction is true. For instance, if $f(n) = n$ and $g(n) = n^2$, $f(n) = O(g(n))$, but $g(n) \neq O(f(n))$. (f) T. By Theorem 5.36. (g) T. By Theorem 5.18. (h) T. By Theorem 5.28.
5.42 $c_1 n^2$; $c_2 n^2$; $\frac{1}{2} - \frac{3}{n}$; $\frac{10-6}{20} = \frac{1}{5}$; $\frac{1}{5} n^2$; $\frac{1}{2} n^2$; 10.
5.43 There are a few ways to think about this. First, the larger n is, the smaller $\frac{3}{n}$ is, so a smaller amount is being subtracted. But that's perhaps too fuzzy. Let's look at it this way:

$$n \geq 10 \Rightarrow \frac{10}{3} \leq \frac{n}{3} \Rightarrow \frac{3}{n} \leq \frac{3}{10} \Rightarrow -\frac{3}{n} \geq -\frac{3}{10} \Rightarrow \frac{1}{2} - \frac{3}{n} \geq \frac{1}{2} - \frac{3}{10}.$$

5.45 (a) Theorem 5.18. (b) Absolutely not! Theorem 5.18 requires that we also prove $f(n) = \Omega(g(n))$. Here is a counterexample: $n = O(n^2)$, but $n \neq \Theta(n^2)$. So $f(n) = O(g(n))$ does not imply that $f(n) = \Theta(g(n))$.

5.46 Notice that when $n \geq 1$, $n! = 1 \cdot 2 \cdot 3 \cdots n \leq n \cdot n \cdots n = n^n$. Therefore $n! = O(n^n)$ (We used $n_0 = 1$, and $c = 1$.)

5.49 If $f(x) = O(g(x))$, then there are positive constants c_1 and n_0' such that

$$0 \leq f(n) \leq c_1\, g(n) \text{ for all } n \geq n_0',$$

and if $g(x) = O(h(x))$, then there are positive constants c_2 and n_0'' such that

$$0 \leq g(n) \leq c_2\, h(n) \text{ for all } n \geq n_0''.$$

Set $n_0 = \max(n_0', n_0'')$ and $c_3 = c_1\, c_2$. Then

$$0 \leq f(n) \leq c_1\, g(n) \leq c_1\, c_2\, h(n) = c_3\, h(n) \text{ for all } n \geq n_0.$$

Thus $f(x) = O(h(x))$.

5.53 (a) ∞ (b) ∞ (c) ∞ (d) ∞ (e) 0 (f) 0 (g) 8675309

5.57 Theorem 5.51 part (b) implies that $\lim_{n\to\infty} n^2 = \infty$. Since the limit being computed was actually $\lim_{n\to\infty} \dfrac{1}{n^2}$, Theorem 5.55 was used to obtain the final answer of 0 for the limit.

5.58 Notice that $\lim_{x\to\infty} \frac{3x^3}{x^2} = \lim_{x\to\infty} 3x = \infty$, so $3x^3 = \omega(x^2)$ by the second case of the Theorem 5.50, which also implies that $3x^3 = \Omega(x^2)$.

5.63 Notice that $\lim\limits_{n\to\infty} \dfrac{n(n+1)/2}{n^2} = \lim\limits_{n\to\infty} \dfrac{n^2+n}{2n^2} = \lim\limits_{n\to\infty} \dfrac{1}{2} + \dfrac{1}{2n} = \dfrac{1}{2} + 0 = \dfrac{1}{2}$, so $n(n+1)/2 = \Theta(n^2)$.

5.64 (a) Since $\lim\limits_{x\to\infty} \dfrac{2^x}{3^x} = \lim\limits_{x\to\infty} \left(\dfrac{2}{3}\right)^x = 0$, the result follows.

(b) If $x \geq 1$, then clearly $(3/2)^x \geq 1$, so $2^x \leq 2^x \left(\frac{3}{2}\right)^x = \left(\frac{2\times 3}{2}\right)^x = 3^x$. Therefore, $2^x = O(3^x)$.

5.70

Evaluation of Proof 1: 7^x grows faster than 5^x does not mean $7^x - 5^x > 0$ for all $x \neq 0$. For one thing, we are really only concerned about positive values of x. Further, we are specifically concerned about very large values of x. In other words, we want something to be true for all x that are 'large enough'. Also, this statement does not take into account constant factors. Similarly, a tight bound does *not* imply that $7^x - 5^x = 0$. The bottom line: This one is way off. They are not conveying an understanding of what 'upper bound' really means, and they certainly haven't proven anything. Frankly, I don't think they have a clue what they are trying to say in this proof.

Evaluation of Proof 2: This one has several problems. First, the application of l'Hopital's rule is incorrect. The result should be $\lim\limits_{x\to\infty} \dfrac{5^x \log 5}{7^x \log 7}$, which should make it obvious that l'Hopital's rule doesn't actually help in this case. (The key to this one is to do a little algebra.) The next problem is the statement 'but $x \log 7$ gets there faster'. What exactly does that mean? Asymptotically faster, or just faster? If the former, it needs to be proven. If the latter, that isn't enough to prove relative growth rates. Finally, even if this showed that $5^x = O(7^x)$, that only shows that 7^x is an upper bound on 5^x. It does not show that the bound is not tight. The bottom line is that bad algebra combined with vague statements falls way short of a correct proof.

Evaluation of Proof 3: This proof is *very* close to being correct. The main problem is that they only stated that $5^x = O(7^x)$, but they also needed to show that $5^x \neq \Theta(7^x)$. It turns out that

the theorem they mention also gives them that. So all they needed to add is 'and $5^x \neq \Theta(7^x)$' at the end. Technically, there is another problem—they should have taken the limit of $5^x/7^x$. What they really showed using the limit theorem is that $7^x = \omega(5^x)$, which is equivalent to $5^x = o(7^x)$. It isn't a major problem, but technically the limit theorem does not directly give them the result they say it does. If you are trying to prove that $f(x)$ is bounded by $g(x)$, put $f(x)$ on the top and $g(x)$ on the bottom.

5.72 You should have come up with $n^2 \log n$ for the upper bound. If you didn't, now that you know the answer, go back and try to write the proofs before reading them here. (a) If $n > 1$,

$$\ln(n^2+1) \leq \ln(n^2+n^2) = \ln(2n^2) = (\ln 2 + \ln n^2) \leq (\ln n + 2\ln n) = 3\ln n$$

Thus when $n > 1$,

$$n\ln(n^2+1) + n^2 \ln n \leq n3\ln n + n^2 \ln n \leq 3n^2 \ln n + n^2 \ln n \leq 4n^2 \ln n.$$

Thus, $n\ln(n^2+1) + n^2\ln n = O(n^2 \ln n)$. (You may have different algebra in your proof. Just make certain that however you did it that it is correct.)

$$\begin{aligned}
\text{(b)} \quad \lim_{x\to\infty} \frac{n\ln(n^2+1) + n^2\ln n}{n^2 \ln n} &= \lim_{x\to\infty} \frac{n\ln(n^2+1)}{n^2\ln n} + 1 \\
&= 1 + \lim_{x\to\infty} \frac{\ln(n^2+1)}{n\ln n} \\
&= 1 + \lim_{x\to\infty} \frac{\frac{2n}{n^2+1}}{1\cdot \ln n + n\cdot \frac{1}{n}} \qquad \text{(l'Hopital)} \\
&= 1 + \lim_{x\to\infty} \frac{2n}{(n^2+1)(\ln n + 1)} \\
&= 1 + \lim_{x\to\infty} \frac{2}{2n(\ln n + 1) + (n^2+1)\cdot \frac{1}{n}} \qquad \text{(l'Hopital)} \\
&= 1 + \lim_{x\to\infty} \frac{2}{2n(\ln n + 1) + n + \frac{1}{n}} \\
&= 1 + 0 = 1.
\end{aligned}$$

Therefore, $n\ln(n^2+1) + n^2\ln n = \Theta(n^2 \log n)$.

5.74 We can see that $(n^2-1)^5 = \Theta(n^{10})$ since

$$\lim_{n\to\infty} \frac{(n^2-1)^5}{n^{10}} = \lim_{n\to\infty} \left(\frac{n^2-1}{n^2}\right)^5 = \lim_{n\to\infty} \left(1 - \frac{1}{n^2}\right)^5 = 1.$$

5.75 The following limit shows that $2^{n+1} + 5^{n-1} = \Theta(5^n)$.

$$\lim_{n\to\infty} \frac{2^{n+1} + 5^{n-1}}{5^n} = \lim_{n\to\infty} \frac{2^{n+1}}{5^n} + \frac{5^{n-1}}{5^n} = \lim_{n\to\infty} 2\left(\frac{2}{5}\right)^n + \frac{1}{5} = 0 + \frac{1}{5}.$$

Note that we could also have shown that $2^{n+1} + 5^{n-1} = \Theta(5^{n-1})$, but that is not as simple of a function.

5.78 Since $a < b$, $b - a > 0$. Therefore, $\lim_{n\to\infty} \frac{n^a}{n^b} = \lim_{n\to\infty} n^{a-b} = \lim_{n\to\infty} \frac{1}{n^{b-a}} = 0$. By Theorem 5.50, $n^a = o(n^b)$.

5.81 Since $a < b$, $a/b < 1$. Therefore, $\lim_{n\to\infty} \frac{a^n}{b^n} = \lim_{n\to\infty} \left(\frac{a}{b}\right)^n = 0$. By Theorem 5.50, $a^n = o(b^n)$.

5.86 (a) False since 3^n grows faster than 2^n. (b) True since 2^n grows slower than 3^n. (c) False since 3^n grows faster than 2^n, which means it does not grow slower or at the same rate. (d) True since they both have the same growth rate. Remember, exponentials with different bases have different growth rates, but logarithms with different bases have the same growth rate. (e) True since they have the same growth rate. Remember that if $f(n) = \Theta(g(n))$, then $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. (f) False since they have the same growth rate, so $\log_{10} n$ does not grow slower than $\log_3 n$.

5.89 Using l'Hopital's rule, we have $\lim_{n\to\infty} \frac{\log_c(n)}{n^b} = \lim_{n\to\infty} \frac{\frac{1}{n\ln(c)}}{b\,n^{b-1}} = \lim_{n\to\infty} \frac{1}{\ln(c) b\, n^b} = 0$ since $b > 0$. Thus, Theorem 5.50 tells us that $\log_c n = o(n^b)$.

5.94 (a) Θ; (b) o (O is correct, but not precise enough.); (c) Θ; (d) o (O is correct, but not precise enough.); (e) Θ since $2^n = 2\,2^{n-1}$; (f) Ω (Technically it is ω, but I'll let it slide if you put Ω since we haven't used ω much.); (g) through (j) are all o (O is correct, but not precise enough.)

5.96 If your answers do not all start with Θ, go back and redo them before reading the answers. Your answers should match the following *exactly*. (a) $\Theta(n^7)$. (b) $\Theta(n^8)$. (c) $\Theta(n^2)$. (d) $\Theta(3^n)$. (e) $\Theta(2^n)$. (f) $\Theta(n^2)$. (g) $\Theta(n^{.000001})$. (h) $\Theta(n^n)$.

5.97 Here is the correct ranking (where $\sim$ indicates two functions grow at the same rate):
$10000,\ \log x \sim \log(x^{300}),\ \log^{300} x,\ x^{.000001},\ \ x \sim \log(2^x),\ \ x\log(x),\ \ x^{log_2 3},\ \ x^2,\ \ x^5,\ \ 2^x,\ \ 3^x.$

5.99 (a) No. The domain is $\mathbb{Z}$, which does not have a 'starting point'. (b) Yes. The domain is $\mathbb{Z}^+$. (c) Yes. The domain is $\{2, 3, 4, \ldots\}$. (d) Yes. The domain is $\mathbb{Z}^+$. (e) No. The domain is $\mathbb{R}$ which is not a subset of $\mathbb{Z}$. Thus, not only is there no 'starting point,' there is no clear ordering of the real numbers from one to the next.

5.101 Modus ponens.

5.102 You can immediately conclude that $P(6)$ is true using modus ponens. If that was your answer, good. But you can keep going. Since $P(6)$ is true, you can conclude that $P(7)$ is true (also by modus ponens). But then you can conclude that $P(8)$ is true. And so on. The most complete answer you can give is that $P(n)$ is true for all $n \geq 5$. You *cannot* conclude that $P(n)$ is true for all $n \geq 1$ because we don't know anything about the truth values of $P(1)$, $P(2)$, $P(3)$, and $P(4)$.

5.103 Nothing. We can conclude that $P(n)$ is true for any $n \geq 17$, but there is not enough information to say anything about values of n less than 17.

5.104 There are various ways to say this, including what was said in the paragraph above. Here is another way to say it:

> If $P(a)$ is true, and for any value of $k \geq a$, $P(k)$ true implies that $P(k+1)$ is true, then $P(n)$ is true for all $n \geq a$.

5.106 If you answered **yes** and you aren't lying, great! If you answered *no* or you answered **yes** but you lied, it is important that you think about it some more and/or get some help. If you want to succeed at writing induction proofs, understanding this is an important step!

5.109 $\frac{1(1+1)}{2}$; $P(1)$ is true; $P(k)$ is true; $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$; $P(k+1)$; $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$; $\sum_{i=1}^{k} i$; $\frac{k(k+1)}{2}$; $\frac{k}{2} + 1$; $\frac{(k+1)(k+2)}{2}$; $P(k+1)$ is true; $P(1)$ is true; $k \geq 1$; all $n \geq 1$; induction *or* the principle of mathematical induction *or* PMI.

5.110

(a) $P(k)$ is the statement "$\sum_{i=1}^{k} i \cdot i! = (k+1)! - 1$"

(b) $P(k+1)$ is the statement "$\sum_{i=1}^{k+1} i \cdot i! = (k+2)! - 1$"

(c) $LHS(k) = \sum_{i=1}^{k} i \cdot i!$

(d) $RHS(k) = (k+1)! - 1$

(e) $LHS(k+1) = \sum_{i=1}^{k+1} i \cdot i!$

(f) $RHS(k+1) = (k+2)! - 1$

5.113 Define $P(n)$ to be the statement "$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$". We need to show that $P(n)$ is true for all $n \geq 1$.

Base Case: Since $\sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{1(2)(3)}{6}$, $P(1)$ is true. (If your algebra is in a different order, like $\sum_{i=1}^{1} i^2 = \frac{1(2)(3)}{6} = 1$, it is incorrect. We only know that $\sum_{i=1}^{1} i^2 = \frac{1(2)(3)}{6}$ because we first saw that $\sum_{i=1}^{1} i^2 = 1$, and then were able to see that $1 = \frac{1(2)(3)}{6}$.)

Inductive Hypothesis: Let $k \geq 1$ and assume $P(k)$ is true. That is, $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$.

(As a side note, I know that what I need to prove next is

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2(k+1)+1)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}.$$

I am only writing this down now so that I know what my goal is. I am not going to start working both sides of this or otherwise manipulate it. I can't because I don't know whether or not it is true yet.)

Inductive Step: Notice that

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \sum_{i=1}^{k} i^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{k(2k+1)+6(k+1)}{6}\right) \\
&= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right) \\
&= \frac{(k+1)(k+2)(2k+3)}{6}.
\end{aligned}$$

Therefore $P(k+1)$ is true.
Summary: Since $P(1)$ is true and $P(k) \to P(k+1)$ is true when $k \geq 1$, $P(n)$ is true for all $n \geq 1$ by induction.
5.115 For $k = 1$ we have $1 \cdot 2 = 2 + (1-1)2^2$, and so the statement is true for $n = 1$. Let $k \geq 1$ and assume the statement is true for k. That is, assume

$$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + k \cdot 2^k = 2 + (k-1)2^{k+1}.$$

We need to show that

$$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + (k+1) \cdot 2^{k+1} = 2 + k2^{k+2}.$$

Using some algebra and the inductive hypothesis, we can see that

$$\begin{aligned}
1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + k \cdot 2^k + (k+1)2^{k+1} &= 2 + (k-1)2^{k+1} + (k+1)2^{k+1} \\
&= 2 + (k-1+k+1)2^{k+1} \\
&= 2 + 2k2^{k+1} \\
&= 2 + k2^{k+2}.
\end{aligned}$$

Thus, the result is true for $k+1$. The result follows by induction.
5.117 This proof is very close to being correct, but is suffers from a few small but important errors:

- For the sake of clarity, it might have been better to use k throughout most of the proof instead of n. The exception is in the final sentence where n is correct.
- The base case is just some algebra without context. A few words are needed. For instance, 'notice that when $n = 1$,'.

- The base case is presented incorrectly. Notice that the writer starts by writing down what she wants to be true and then deduces that it is indeed correct by doing algebra on both sides of the equation. As we have already mentioned, *you should* **never** *start with what you want to prove and work both sides!* It is not only sloppy, but it can lead to incorrect proofs. Whenever I see students do this, I always tell them to use what I call the U method. What I mean is rewrite your work by starting at the upper left, going down the left side, then doing up the right side. So the above should be rewritten as:

  $$1 \cdot 1! = 1 = 2! - 1 = (1+1)! - 1.$$

  Notice that if the U method does not work (because one or more steps isn't correct), it is probably an indication of an incorrect proof. Consider what happens if you try it on the proof in Exercise 2.91. You would write $-1 = (-1)^2 = 1 = 1^2 = 1$. Notice that the first equality is incorrect.

  The U method can sometimes apply to inequalities as well.

- When the writer makes her assumption, she says 'for $n \geq 1$'. This is O.K., but there is some ambiguity here. Does she mean for *all* n, or for a particular value of n? She must mean the latter since the former is what she is trying to prove. It would have been better for her to say 'for some $n \geq 1$.'

- The algebra in the inductive step is perfect. However, what does it mean? She should include something like 'Notice that' before her algebra just to give it a little context. It often doesn't take a lot of words, but adding a few phrases here and there goes a long way to help a proof flow more clearly.

- She says 'Therefore it is true for n'. She must have meant $n+1$ since that is what she just proved.

- As with her assumption, her final statement could be clarified by saying 'for all $n \geq 1$.'

Overall, the proof has almost all of the correct content. Most of the problems have to do with presentation. But as we have seen with other types of proofs, the details are really important to get right!

5.118 Given this proof, we know that $P(1)$ is true. We also know that $P(2) \to P(3)$, $P(3) \to P(4)$, etc, are all true. Unfortunately, the proof omits showing that $P(2)$ is true, so modus ponens never applies. In other words, knowing that $P(2) \to P(3)$ is true does us no good unless we know $P(2)$ is true, which we don't. Because of this, we don't know anything about the truth values of $P(3)$, $P(4)$, etc. The proof either needs to show that $P(2)$ is true as part of the base case, or the inductive step needs to start at 1 instead of 2.

5.120 Because our inductive hypothesis was that $P(k-1)$ is true instead of $P(k)$. If we assumed that $k \geq 0$, then when $k = 0$ it would mean we are assuming $P(-1)$ is true, and we don't know whether or not it is since we never discussed $P(-1)$.

5.124 This contains a very subtle error. Did you find it? If not, go back and carefully re-read the proof and think carefully–at least one thing said in the proof *must* be incorrect. What is it?

O.K., here it is: The statement 'goat 2 is in both collections' is not always true. If $n = 1$, then the first collection contains goats 1 through 1, and the second collection contains goats 2 through 2. In this case, there is no overlap of goat 2, so the proof falls apart.

5.125

Evaluation of Proof 1: This solution is on the right track, but it has several technical problems.

- The base case should be $k = 0$, not $k = 1$.
- The way the base case is worded could be improved. For instance, what purpose does saying '$2 = 2$' serve? Also, the separate sentence that just says 'it is true' is a little vague and awkward. I would reword this as:

  > The total number of palindromes of length $2 \cdot 1$ is $2 = 2^1$, so the statement is true for $k = 1$.

  Of course, the base case should *really* be $k = 0$, but if it were $k = 1$, that is how I would word it.
- The connection between palindromes of length $2k$ and $2(k + 1)$ is not entirely clear and is incorrect as stated. A palindrome of length $2(k+1)$ can be formed from a palindrome of length $2k$ by adding a 0 to both the beginning and end or adding a 1 to both the beginning and the end. This what was probably meant, but it is not what the proof actually says.

  But we need to say a little more about this. Every palindrome of length $2(k + 1)$ can be formed from exactly one palindrome of length $2k$ with this method. But is this enough? Not quite. We also need to know that every palindrome of length $2k$ can be extended to a palindrome of length $2(k+1)$, and it should be clear that this is the case. In summary, the inductive step needs to establish that there are twice as many binary palindromes of length $2(k + 1)$ as there are of length $2k$. The argument has to convince the reader that there is a 2-to-1 correspondence between these sets of palindromes. In other words, we did not omit or double-count any.

Evaluation of Proof 2: The base case correct. Unfortunately, that is about the only thing that is correct.

- The second sentence is wrong. We cannot say that 'it is true for all n'–that is precisely what we are trying to prove. We need to assume it is true for a *particular* n and then prove it is true for $n + 1$.
- The rest of the proof is one really long sentence that is difficult to follow. It should be split into much shorter sentences, each of which provides one step of the proof.
- The term 'binary number' should be replaced with 'binary palindrome' throughout. It causes confusion, especially when the words 'add' and 'consecutive' are used. These mean something very different if we have numbers in mind instead of strings.
- I don't think the phrase 'each consecutive binary number' means what the writer thinks it means. The binary numbers 1001 and 1010 are consecutive (representing 9 and 10), but that is probably *not* what the writer has in mind.
- The term 'permutations' shows up for some reason. I think they might have mean 'strings' or something else.
- Why bring up the 4 possible ways to extend a binary string by adding to the beginning and end if only two of them are relevant? Why not just consider the ones of interest in the first place?
- In the context of a proof, the phrase 'you are adding' doesn't make sense. Why am I adding something and what am I adding it to? And do they mean addition (of the binary numbers) or appending (of strings)?

- They switch from n to k in the middle of the proof to provide further confusion.

Evaluation of Proof 3: This proof has most of the right ideas, but it does not put them together well. The base case is correct. It sounds like the writer understands what is going on with the inductive step, but needs to communicate it more clearly. More specifically, what does 'assume $2k \to 2^k$ palindromes' mean? I think I am supposed to read this as 'assume that there are 2^k palindromes of length $2k$.' [1]

The final sentence is also problematic. The first phrase tries to connect to the previous sentence, but the connection needs to be a little more clear. The final phrase is not a complete thought. In the first place, I know that $2^k + 2^k = 2^{k+1}$ and this has nothing to do with the previous phrases. In other words, the 'so' connecting the phrases doesn't make sense. But more seriously, why do I care that $2^k + 2^k = 2^{k+1}$? What he meant was something like 'so there are $2^k + 2^k = 2^{k+1}$ palindromes of length $2k + 2$'.

5.126 The empty string is the only string of length 0, and it is a palindrome. Thus there is $1 = 2^0$ palindromes of length 0.

Now assume there are 2^n binary palindromes of length $2n$. For every palindrome of length $2n$, exactly two palindromes of length $2(n + 1)$ can be constructed by appending either a 0 or a 1 to both the beginning and the end. Further, every palindrome of length $2(n + 1)$ can be constructed this way. Thus, there are twice as many palindromes of length $2(n + 1)$ as there are of length $2n$. By the inductive hypothesis, there are $2 \cdot 2^n = 2^{n+1}$ binary palindromes of length $2(n + 1)$.

The result follows by PMI.

5.130 (a) $r_{n/2}$. (b) 1. (c) $a_{n-1} + 2 \cdot a_{n-2} + 3 \cdot a_{n-3} + 4 \cdot a_{n-4}$. (d) There are none.

5.134 It means to find a closed-form expression for it. In other words, one that does not define the sequence recursively.

5.136 When $n = 1$, $T(1) = 1 = 0+1 = \log_2 1+1$. Assume that $T(k) = \log_2 k+1$ for all $1 \leq k < n$ (we are using strong induction). Then

$$\begin{aligned} T(n) &= T(n/2) + 1 \\ &= (\log_2(n/2) + 1) + 1 \\ &= \log_2 n - \log_2 2 + 2 \\ &= \log_2 n - 1 + 2 \\ &= \log_2 n + 1. \end{aligned}$$

So by PMI, $T(n) = \log_2 n + 1$ for all $n \geq 1$.

5.138 We begin by computing a few values to see if we can find a pattern. $A(2) = A(1) + 2 = 2 + 2 = 4$, $A(3) = A(2) + 2 = 4 + 2 = 6$, $A(4) = 8$, $A(5) = 10$, etc. It seems pretty obvious that $A(n) = 2n$. It holds for $n = 1$, so we have our base case. Assume $A(n) = 2n$. Then $A(n + 1) = A(n) + 2 = 2n + 2 = 2(n + 1)$, so it holds for $n + 1$. By PMI, $A(n) = 2n$ for all $n \geq 1$.

5.140 It contains 3 very different looking recursive terms so it is very unlikely we will be able to find any sort of meaningful pattern by iteration.

[1] In general, avoid the use of mathematical symbols in constructing the grammar of an English sentence. One of the most common abuses I see is the use of $\to$ in the middle of a sentence.

5.142

$$\begin{aligned} H(n) &= 2H(n-1)+1 \\ &= 2(2H(n-2)+1)+1 \\ &= 2^2H(n-2)+2+1 \\ &= 2^2(2H(n-3)+1)+2+1 \\ &= 2^3H(n-3)+2^2+2+1 \\ &\vdots \\ &= 2^{n-1}H(1)+2^{n-2}+2^{n-3}+\cdots+2+1 \\ &= 2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2+1 \\ &= 2^n-1 \end{aligned}$$

Thus, $H(n) = 2^n - 1$. Luckily, this matches our answer from Example 5.137.

5.144 Iterating a few steps, we discover:

$$\begin{aligned} T(n) &= T(n/2)+1 \\ &= T(n/4)+1+1 \\ &= T(n/2^2)+2 \quad \text{(I think I see a pattern!)} \\ &= T(n/2^3)+1+2 \\ &= T(n/2^3)+3 \quad \text{(I } \textit{do} \text{ see a pattern!)} \\ &\vdots \\ &= T(n/2^k)+k \end{aligned}$$

We need to find k such that $n/2^k = 1$. We already saw in Example 5.141 that $k = \log_2 n$ is the solution. Therefore, we have

$$\begin{aligned} T(n) &= T(n/2^k)+k \\ &= T(n/2^{\log_2 n})+\log_2 n \\ &= T(1)+\log_2 n \\ &= 1+\log_2 n \end{aligned}$$

Therefore, $T(n) = 1 + \log_2 n$.

5.145 The final answer is $T(n) = 2^{n+1} - n - 2$ or $T(n) = 4 \cdot 2^{n-1} - n - 2$. It is important that you can work this out yourself, so try your best to get this answer without looking further. But if you get stuck or have a different answer, you can refer to the following skeleton of steps–we have omitted many of the steps because we want you to work them out. It does provide a few reference

points along the way, however.

$$\begin{aligned}
T(n) &= 2T(n-1)+n \\
&= 2(2T(n-2)+(n-1))+n \text{ (having } n \text{ instead of } (n-1) \text{ is a common error)} \\
&= 2^2T(n-2)+3n-2 \text{ (it is unclear yet if I should have } 3n-2 \text{ or some other form)} \\
&\vdots \quad \text{(many skipped steps)} \\
&= 2^kT(n-k)+(2^k-1)n-\sum_{i=1}^{k-1} i2^i \text{ (the all-important pattern revealed)} \\
&\vdots \quad \text{(plug in appropriate value of } k \text{ and simplify)} \\
&= 2^{n+1}-n-2.
\end{aligned}$$

5.149 Here we have $a = 1$, $b = 2$, and $d = 0$. Since $1 = 2^0$, the second case of the Master Theorem tells is that $T(n) = \Theta(n^0 \log n) = \Theta(\log n)$. Since we have already seen several times that $T(n) = \log_2 n + 1$, we can notice that this answer is consistent with those. It's a good thing.

5.151 Here, $a = 2, b = 2$, and $d = 0$. ($d = 0$ since $1 = 1 \cdot n^0$. In general, $c = c \cdot n^0$, so when $f(n)$ is a constant, $d = 0$.) Since $a > 2^0$, we have $T(n) = \Theta(n^{\log_a a}) = \Theta(n^1) = \Theta(n)$ by the third case of the Master Theorem.

5.153 We have $a = 7$, $b = 2$, and $d = 2$. Since $7 > 2^2$, the third case of the Master Theorem applies so $T(n) = \Theta(n^{\log_2 7})$, which is about $\Theta(n^{2.8})$.

5.154 Because it isn't true. Although the growth rate of $n^{\log_2 7}$ and $n^{2.8}$ are close, they are not exactly the same, so $\Theta(n^{\log_2 7}) \neq \Theta(n^{2.8})$. We *could* say that $T(n) = \Theta(n^{\log_2 7}) = O(n^{2.81})$, but then we have lost the 'tightness' of the bound. And I want to be able to say "Yo dawg, that bound is really *tight*!"

5.160 By raising the subscripts in the homogeneous equation we obtain the characteristic equation $x^n = 9x^{n-1}$ or $x = 9$. A solution to the homogeneous equation will be of the form $x_n = A(9)^n$. Now $f(n) = -56n + 63$ is a polynomial of degree 1 and so we assume that the solution will have the form $x_n = A9^n + Bn + C$. Now $x_0 = 2, x_1 = 9(2) - 56 + 63 = 25, x_2 = 9(25) - 56(2) + 63 = 176$. We thus solve the system

$$\begin{aligned}
2 &= A + C, \\
25 &= 9A + B + C, \\
176 &= 81A + 2B + C.
\end{aligned}$$

We find $A = 2, B = 7, C = 0$, so the solution is $x_n = 2(9^n) + 7n$.

5.164 The characteristic equation is $x^2 - 4x + 4 = (x-2)^2 = 0$. There is a multiple root and so we must test a solution of the form $x_n = A2^n + Bn2^n$. The initial conditions give

$$\begin{aligned}
1 &= A, \\
4 &= 2A + 2B.
\end{aligned}$$

This solves to $A = 1, B = 1$. The solution is thus $x_n = 2^n + n2^n$.

6.4 Nobody in their right mind will choose fruit if cake and ice cream are available, so there are $3 + 8 = 11$ choices. Just kidding. There are really $3 + 8 + 5 = 16$ different choices.

6.7 There are 26 choices for each of the first three characters, and 10 choices for each of the final three characters. Therefore, there are $26^3 \cdot 10^3$ possible license plates.

6.10 Every divisor of n is of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $0 \leq b_1 \leq a_1$, $0 \leq b_2 \leq a_2$, …, $0 \leq b_k \leq a_k$. (We could also write this as $0 \leq b_i \leq a_i$ for $0 \leq i \leq k$.) Therefore there are $a_1 + 1$ choices for b_1,

a_2+1 choices for b_2, all the way through a_k+1 choices for b_k. Since each of the b_is are independent of each other, the product rule tells us that the number of divisors of n is $(a_1+1)(a_2+1)\cdots(a_k+1)$.

6.11 Unless the p_i are distinct, the b_is are not independent of each other. In other words, if the p_is are distinct, then each different choice of the b_is will produce a different number. But this is not the case if the p_is are not distinct. For instance, if we write $32 = 2^3 2^2$, we can get the factor 4 as $2^2 2^0$, $2^1 2^1$, or $2^0 2^2$. Clearly we would count 4 three times and would obtain the incorrect number of divisors.

6.13 Write $n = \underbrace{1+1+\cdots+1}_{n-1\ +'\text{s}}$. There are two choices for each plus sign–leave it or perform the addition. Each of the 2^{n-1} ways of making choices leads to a different expression, and every expression can be constructed this way. Therefore, there are 2^{n-1} such ways of expressing n.

6.15 This combines the product and sum rules. We now have $10 + 26 = 36$ choices for each character, and there are 5 characters, so the answer is 36^5.

6.16 Each bit can be either 0 or 1, so there are 2^n bit strings of length n.

6.18 $53 \cdot 63^2$; $53 \cdot 63^3$; $53 \cdot 63^{k-1}$.

6.21 It contains at least one repeated digit. The wording of your answer is very important. Your answer should not be "it has some digit twice" since this is vague–do you mean 'exactly twice'? If so, that is incorrect. If you mean 'at least twice', then it is better to be explicit and say it that way or just say 'repeated'. To be clear, we don't know that it contains any digit exactly twice, and we also don't know how many unique digits the number has–it might be 22222222222, but it also might be 98765432101.

6.24 If all the magenta, all the yellow, all the white, 14 of the red and 14 of the blue marbles are drawn, then in among these $8 + 10 + 12 + 14 + 14 = 58$ there are no 15 marbles of the same color. Thus we need 59 marbles in order to insure that there will be 15 marbles of the same color.

6.25 She knows that you are the 25th person in line. If everyone gets 4 tickets, she will get none, but you will get the 4 you want. She can get one or more tickets if one or more people in front of her, including you, get less than 4.

6.28 There are seven possible sums, each one a number in $\{-3, -2, -1, 0, 1, 2, 3\}$. By the Pigeonhole Principle, two of the eight sums must add up to the same number.

6.31 We have $\lceil \frac{16}{5} \rceil = 4$, so some cat has at least four kittens.

6.32

Evaluation of Proof 1: This proof is incomplete. It kind of argues it for 5, not n in general. Even then, the proof is neither clear not complete. For instance, what are the 4 'slots'?

Evaluation of Proof 2: They only prove it for $n = 2$. It needs to be proven for *any* n.

Evaluation of Proof 3: You can't assume somebody had shaken hands with everyone else without some justification. You certainly can't assume it was any particular person (i.e. person n). Similarly, you can't assume the next person has shaken $n-2$ hands without justifying it. The final statement is weird (what does 'fulfills the contradiction' mean?) and needs justification (why is it a problem that the last person shakes no hands?).

6.33 Notice that if someone shakes $n-1$ hands, then nobody shakes 0 hands and vice-verse. Thus, we have two cases. If someone shakes $n-1$ hands, then the n people can shake hands with between 1 and $n-1$ other people. If nobody shakes hands with $n-1$ people, then the n people can shake hands with between 0 and $n-2$ other people. In either case, there are $n-1$ possibilities for the number of hands that the n people can shake. The pigeonhole principle implies that two people shake hands with the same number of people.

Note: You cannot say that the two cases are that someone shakes hands with $n-1$ or someone shakes hands with 0. It may be that *neither* of these is true. The two cases are someone shakes hands with $n-1$ others or nobody does. Alternatively, you could say someone shakes hands with 0 others or nobody does.

6.34 Choose a particular person of the group, say Charlie. He corresponds with sixteen others. By the pigeonhole principle, Charlie must write to at least six of the people about one topic, say topic I. If any pair of these six people corresponds about topic I, then Charlie and this pair do the trick, and we are done. Otherwise, these six correspond amongst themselves only on topics II or III. Choose a particular person from this group of six, say Eric. By the Pigeonhole Principle, there must be three of the five remaining that correspond with Eric about one of the topics, say topic II. If amongst these three there is a pair that corresponds with each other on topic II, then Eric and this pair correspond on topic II, and we are done. Otherwise, these three people only correspond with one another on topic III, and we are done again.

6.38 EAT, ETA, ATE, AET, TAE, and TEA.

6.41 Since there are 15 letters and none of them repeat, there are 15! permutations of the letters in the word UNCOPYRIGHTABLE.

6.43 (a) $5 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 25,200$. (b) We condition on the last digit. If the last digit were 1 or 5 then we would have 5 choices for the first digit and 2 for the last digit. Then there are 6 left to choose from for the second, 5 for the third, etc. So this leads to

$$5 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 2 = 7,200$$

possible phone numbers. If the last digit were either 3 or 7, then we would have 4 choices for the first digit and 2 for the last. The rest of the digits have the same number of possibilities as above, so we would have

$$4 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 2 = 5,760$$

possible phone numbers. Thus the total number of phone numbers is

$$7200 + 5760 = 12,960.$$

6.45 Label the letters T_1, A_1, L_1, and L_2. There are 4! permutations of these letters. However, every permutation that has L_1 before L_2 is actually identical to one having L_1 before L_2, so we have double-counted. Therefore, there are $4!/2 = 12$ permutations of the letters in $TALL$.

6.46 $TALL$, $TLAL$, $TLLA$, $ATLL$, $ALTL$, $ALLT$, $LLAT$, $LALT$, $LATL$, $LLTA$, $LTLA$, and $LTAL$. That makes 12 permutations, which is exactly what we said it should be in Exercise 6.45.

6.47 Following similar logic to the previous few examples, since we have one letter that is repeated three times, and a total of 5 letters, the answer is $5!/3! = 20$.

6.48 Ten of them are $AIEEE$, $AEIEE$, $AEEIE$, $AEEEI$, $EAIEE$, $EAEIE$, $EAEEI$, $EEAIE$, $EEAEI$, $EEEAI$. The other ten are identical to these, but with the A and I swapped.

6.51 We can consider $SMITH$ as one block along with the remaining 5 letters A, L, G, O, and R. Thus, we are permuting 6 'letters', all of which are unique. So there are $6! = 720$ possible permutations.

6.54 (a) $5 \cdot 8^6 = 1310720$. (b) $5 \cdot 8^5 \cdot 4 = 655360$. (c) $5 \cdot 8^5 \cdot 4 = 655360$.

6.58 (a) $\dfrac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 21$. (b) $\dfrac{12 \cdot 11}{1 \cdot 2} = 66$. (c) $\dfrac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 252$.
(d) $\dfrac{200 \cdot 199 \cdot 198 \cdot 197}{1 \cdot 2 \cdot 3 \cdot 4} = 64,684,950$. (e) 1.

6.61 (a) $\binom{17}{15} = \binom{17}{2} = \dfrac{17 \cdot 16}{1 \cdot 2} = 136$. (b) $\binom{12}{10} = \binom{12}{2} = \dfrac{12 \cdot 11}{1 \cdot 2} = 66$.

(c) $\binom{200}{196} = \binom{200}{4} = \frac{200 \cdot 199 \cdot 198 \cdot 197}{1 \cdot 2 \cdot 3 \cdot 4} = 64,684,950.$ (d) $\binom{67}{66} = \binom{67}{1} = 67/1 = 67.$

6.65 $12, 13, 14, 15, 23, 24, 25, 34, 35, 45.$

6.68

Evaluation of Solution 1: This solution does not take into account which woman was selected and which 15 of the original 16 are left, so this is not correct.

Evaluation of Solution 2: This solution has two problems. First, it counts things multiple times. For instance, any selection that contains both Sally and Kim will be counted twice–once when Sally is the first woman selected and again when Kim is selected first. Second, the product rule should have been used instead of the sum rule. Of course, that hardly matters since it would have been wrong anyway.

Evaluation of Solution 3: This solution is correct.

6.70 To count the number of shortest routes from A to B that pass through point O, we count the number of paths from A to O (of which there are $\binom{5}{3} = 10$) and the number of paths from O to B (of which there are $\binom{4}{3} = 4$). Using the product rule, the desired number of paths is $\binom{5}{3}\binom{4}{3} = 10 \cdot 4 = 40.$

6.71

Evaluation of Solution 1: This answer is incorrect since it will count some of the committees multiple times. If you did not come up with an example of something that gets counted multiple times, you should do so to convince yourself that this answer is incorrect.

Evaluation of Solution 2: This solution is incorrect since it does not take into account which man and woman were selected and which 14 of the original 16 are left.

6.72 There are $\binom{16}{5}$ possible committees. Of these, $\binom{9}{5}$ contain only men and $\binom{7}{5}$ contain only women. Clearly these two sets of committees do not overlap. Therefore, the number of committees that contain at least one man and at least one woman is $\binom{16}{5} - \binom{9}{5} - \binom{7}{5}$.

6.73 Because we subtracted the size of both of these from the total number of possible committees. If the sets intersected, we would have subtracted some possibilities twice and the answer would have been incorrect.

6.75

Evaluation of Solution 1: This solution is incorrect since it double counts some of the possibilities.

Evaluation of Solution 2: This solution is incorrect because it does not take into account the requirement that one course from each group must be taken.

6.76

Evaluation of Solution 1: This solution is incorrect since it counts some of the possibilities multiple times.

Evaluation of Solution 2: This solution is incorrect because it does not take into account the requirement that one course from each group must be taken.

6.79 Using 10 bars to separate the meat and 3 stars to represent the slices, we can see that this is exactly the same as the previous two examples. Thus, the solution is $\binom{13}{10} = \binom{13}{3} = 286$.

6.84

$$\begin{aligned}(2x-y^2)^4 &= \binom{4}{0}(2x)^4 + \binom{4}{1}(2x)^3(-y^2) + \binom{4}{2}(2x)^2(-y^2)^2 + \binom{4}{3}(2x)(-y^2)^3 + \binom{4}{4}(-y^2)^4 \\ &= (2x)^4 + 4(2x)^3(-y^2) + 6(2x)^2(-y^2)^2 + 4(2x)(-y^2)^3 + (-y^2)^4 \\ &= 16x^4 - 32x^3y^2 + 24x^2y^4 - 8xy^6 + y^8\end{aligned}$$

6.85

$$\begin{aligned}(\sqrt{3}+\sqrt{5})^4 &= (\sqrt{3})^4 + 4(\sqrt{3})^3(\sqrt{5}) + 6(\sqrt{3})^2(\sqrt{5})^2 + 4(\sqrt{3})(\sqrt{5})^3 + (\sqrt{5})^4 \\ &= 9 + 12\sqrt{15} + 90 + 20\sqrt{15} + 25 \\ &= 124 + 32\sqrt{15}\end{aligned}$$

6.87 Using a little algebra and the binomial theorem, we can see that

$$\sum_{k=1}^{n}\binom{n}{k}3^k = \sum_{k=0}^{n}\binom{n}{k}3^k - 1 = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}3^k - 1 = (1+3)^n - 1 = 4^n - 1.$$

6.91 Let A be the set of camels eating wheat and B be the set of camels eating barley. We know that $|A| = 46$, $|B| = 57$, and $|A \cup B| = 100 - 10 = 90$. We want $|A \cap B|$. By Theorem 6.89 (solving it for $|A \cap B|$),

$$|A \cap B| = |A| + |B| - |A \cup B| = 46 + 57 - 90 = 13.$$

6.95 Using Theorem 6.93, we know that $28 + 29 + 19 - 14 - 10 - 12 + 8 = 48\%$ watch at least one of these sports. That leaves 52% that don't watch any of them.

6.96 Let C denote the set of people who like candy, I the set of people who like ice cream, and K denote the set of people who like cake. We are given that $|C| = 816$, $|I| = 723$, $|K| = 645$, $|C \cap I| = 562$, $|C \cap K| = 463$, $|I \cap K| = 470$, and $|C \cap I \cap K| = 310$. By Inclusion-Exclusion we have

$$\begin{aligned}|C \cup I \cup K| &= |C| + |I| + |K| \\ &\quad -|C \cap I| - |C \cap K| - |I \cap C| \\ &\quad +|C \cap I \cap K| \\ &= 816 + 723 + 645 - 562 - 463 - 470 + 310 \\ &= 999.\end{aligned}$$

The investigator miscounted, or probably did not report one person who may not have liked any of the three things.

6.98 We can either use inclusion-exclusion for four sets or use a few applications of inclusion-exclusion for two sets. Let's try the latter.

Let A denote the set of those who lost an eye, B denote those who lost an ear, C denote those who lost an arm and D denote those losing a leg. Suppose there are n combatants. Then

$$\begin{aligned}n &\geq |A \cup B| \\ &= |A| + |B| - |A \cap B| \\ &= .7n + .75n - |A \cap B|,\end{aligned}$$

$$\begin{aligned}n &\geq |C \cup D| \\ &= |C| + |D| - |C \cap D| \\ &= .8n + .85n - |C \cap D|.\end{aligned}$$

This gives

$$|A \cap B| \geq .45n,$$

$$|C \cap D| \geq .65n.$$

This means that

$$\begin{array}{rcl} n & \geq & |(A \cap B) \cup (C \cap D)| \\ & = & |A \cap B| + |C \cap D| - |A \cap B \cap C \cap D| \\ & \geq & .45n + .65n - |A \cap B \cap C \cap D|, \end{array}$$

whence

$$|A \cap B \cap C \cap D| \geq .45 + .65n - n = .1n.$$

This means that at least 10% of the combatants lost all four members.

7.24 *abed* is a cycle of length 4 and *ecdab* is a cycle of length 5. Other answers are possible. There is no cycle of length 6 since there are only 5 vertices in the graph and a cycle cannot repeat a vertex.

7.27 You should have drawn something like this (but probably bigger and with dots on the corners): □ △

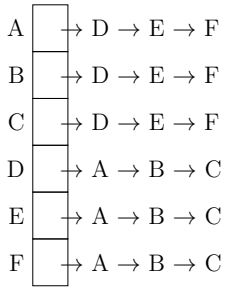
7.30 You should have drawn something like this (but probably bigger and with dots on the corners and center): ×

7.31 You should have drawn a path of length 2 and 4 vertices not connected to anything. Something like this: | . . . .

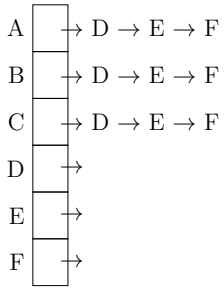
7.47 (a) Yes. Put the vertices on opposite corners in the same set. (b) No. Every other vertex needs to be in the opposite set, and since there is an odd cycle, eventually we get to a situation where a vertex can't be in either set. (c) No. None of the vertices can be in a set with any others since they are all connected to each other. (d) Yes. If I put $000, 110, 011, 101$ in one set and the others in the other set, you can easily see that all of the edges go between sets. (e) Yes. Since it is just a path, put every other vertex in the opposite set. Unlike the situation with the odd cycle, we don't ever loop back so no problems can arise.

7.48 It is true. Notice that a tree with 2 vertices is clearly bipartite since it is just an edge. Assume all trees with n vertices are bipartite, where $n \geq 2$. Let T be a tree with $n+1$ vertices and v be a leaf connected to some vertex u. Let T' be the tree T with the leaf v removed. Then by in the inductive hypothesis, T' is bipartite since it has n vertices. Then T is bipartite since we can put v in the opposite set of u with no risk of edges between the nodes within that set since v is only connected to u. Thus, by PMI, all trees with $n > 2$ vertices are bipartite.

7.57



7.58



7.63

	A	B	C	D	E	E
A	0	0	0	1	1	1
B	0	0	0	1	1	1
C	0	0	0	1	1	1
D	1	1	1	0	0	0
E	1	1	1	0	0	0
F	1	1	1	0	0	0

7.64

	A	B	C	D	E	E
A	0	0	0	1	1	1
B	0	0	0	1	1	1
C	0	0	0	1	1	1
D	0	0	0	0	0	0
E	0	0	0	0	0	0
F	0	0	0	0	0	0

7.75 Did you draw a triangle with a vertex in the middle connected to the three vertices of the triangle? I thought so!

7.81 Notice that $K_{3,3}$ does not have C_3 as a subgraph. Since $K_{3,3}$ has $3 \cdot 3 = 9$ edges and $9 > 8 = 2(6) - 4$, Theorem 7.79 part (b) implies that $K_{3,3}$ is not planar.

7.91 Since C is the set of edges of a connected component of $G_A = (V, A)$, then A has no edges between vertices of C and vertices of $V - C$.

Another way to think about it: If the cut $(C, V - C)$ does not respect A, then there is some $(u, v) \in A$ such that $u \in C$ and $v \in V - C$. But C is the set of edges of a ***connected*** component, and since $(u, v) \in A$, $v \in C$, contradicting the fact that $v \in V - C$. Therefore, the cut $(C, V - C)$ respects A.

7.94 Since Idea 1 is considering adding edges adjacent to a given vertex, Prim's algorithm is essentially using this idea, at least in the first step. Although to be fair, Prim's algorithm is also essentially directly using Theorem 7.90, where C is the single tree it is growing.

On the other hand, Idea 2 is about using minimum weight edges without a specific endpoint in mind, which is what Kruskal's algorithm is doing.

7.97 Recall that the maximum number of edges a graph can have is $m \leq \binom{n}{2} = \frac{n(n-1)}{2} = O(n^2)$. Therefore, $O(\log m) = O(\log n^2) = O(2 \log n) = O(\log n)$. Given this, it is clear that $O(m \log m) = O(m \log n)$

7.102 Lines 1-3 and 6-7 take constant time. Lines 4-5 line takes $O(n)$ time since we are doing n things that take constant time. Line 8 takes $O(n)$ time. The `While` loop executes n times, each time calling `Q.extractMin` that takes $O(\log n)$ and the `ForAll` loop. The code in the `ForAll` loop takes $O(\log n)$ time, and it executes at most $n-1$ times (since there can be at most $n-1$ vertices adjacent

to a given vertex). Combining this together, the complexity is $O(n) + O(n(\log n + (n-1)\log n)) = O(n^2 \log n)$ (Make sure you understand how I simplified this!).

Unfortunately, this actually overestimates the time complexity of the algorithm. Obtaining a better bound takes a little thought and can be tricky to understand, so read carefully! Let's analyze the `ForAll` loop more carefully. In particular, instead of counting up the operations according to how the code is written (iterating over adjacency lists), we will think about how many times the code inside that loop executes in total regardless of when it happens. Notice that the code in the `ForAll` loop can execute at most two times for every edge–once from each endpoint. If you cannot see why this is, definitely ask about it in class! Thus, the complexity of the `ForAll` loop is actually $O(m \log n)$ over all of the iterations of the `While` loop. So the complexity of the `While` loop is $O(m \log n)$ plus the complexity of the `Q.extractMin` method called n times, which we saw was $O(n \log n)$. Given that, the complexity of the algorithm is $O(n) + O(m \log n) + O(n \log n) = O(m \log n)$.

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Index