

MATH 208: DISCRETE MATHEMATICS



DEPARTMENT OF MATHEMATICS AND STATISTICS

University of North Dakota

Copyright © 2025 UND Math Department

Published by UND MATH Department

<http://arts-sciences.und.edu/math//>

Copyright © 2005, 2014, 2023, 2025 University of North Dakota Mathematics Department

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".

Fifth edition, July 2025

This book is dedicated to: Professor Emeritus Jerry Metzger (1944-2024)

TABLE OF CONTENTS

Introduction.....	6
PART I: Logic, Sets, Proof.....	8
Chapter 1: Logical Connectives and Compound Propositions	8
Chapter 2: Logical Equivalence.....	15
Chapter 3: Predicates and Quantifiers.....	20
Chapter 4: Rules of Inference	25
Chapter 5: Sets: Basic Definitions	32
Chapter 6: Set Operations	37
Chapter 7: Styles of Proof.....	44
PART II: Relations and Functions	51
Chapter 8: Relations.....	51
Chapter 9: Properties of Relations	58
Chapter 10: Equivalence Relations	63
Chapter 11: Functions and Their Properties	69
Chapter 12: Special Functions	76
Chapter 13: Sequences and Summations	81
PART III: Recursion, Induction and Algorithms.....	88
Chapter 14: Recursively Defined Sequences	88
Chapter 15: Recursively Defined SetsAn Ancient Song	91
Chapter 16: Mathematical Induction	96
Chapter 17: Algorithms.....	105
Chapter 18: Algorithm Efficiency	111
Chapter 19: The Growth of Functions	115
PART IV: Elementary Number Theory	118
Chapter 20: The Integers.....	118
Chapter 21: The Divides Relation and Primes.....	121
Chapter 22: GCD's and the Euclidean Algorithm	125
Chapter 23: GCD's Reprised	129

Chapter 24: The Fundamental Theorem of Arithmetic.....	134
Chapter 25: Linear Diophantine Equations	137
Chapter 26: Modular Arithmetic	141
Chapter 27: Integers in Other Bases	148
PART V: Counting and Recurrences	153
Chapter 28: The Fundamental Counting Principles.....	153
Chapter 29: Permutations and Combinations	160
Chapter 30: The Binomial Theorem and Pascal's Triangle.....	165
Chapter 31: Inclusion/Exclusion Counting.....	173
Chapter 32: The Pigeonhole Principle	178
Chapter 33: Tougher Counting Problems	182
Chapter 34: Counting Using Recurrence Relations	189
Chapter 35: Solutions to Recurrence Relations	196
Chapter 36: The Method of Characteristic Roots	199
Chapter 37: Solving Non-homogeneous Recurrence Relations.....	205
PART VI: Graph Theory	209
Chapter 38: Graph Isomorphism.....	209
Chapter 39: Paths	219
Chapter 40: Trees.....	225
Appendix A: Solutions to Exercises	230
Chapter 1 Solutions:.....	230
Chapter 2 Solutions:.....	232
Chapter 3 Solutions:.....	235
Chapter 4 Solutions:.....	236
Chapter 5 Solutions:.....	238
Chapter 6 Solutions:.....	239
Chapter 7 Solutions:.....	240
Chapter 8 Solutions:.....	243
Chapter 9 Solutions:.....	244

Chapter 10 Solutions:.....	245
Chapter 11 Solutions:.....	249
Chapter 12 Solutions:.....	250
Chapter 13 Solutions:.....	253
Chapter 14 Solutions:.....	254
Chapter 15 Solutions:.....	255
Chapter 16 Solutions:.....	256
Chapter 20 Solutions:.....	259
Chapter 21 Solutions:.....	260
Chapter 22 Solutions:.....	261
Chapter 23 Solutions:.....	263
Chapter 24 Solutions:.....	264
Chapter 25 Solutions:.....	265
Chapter 26 Solutions:.....	266
Chapter 27 Solutions:.....	268
Chapter 28 Solutions:.....	270
Chapter 29 Solutions:.....	271
Chapter 30 Solutions:.....	272
Chapter 31 Solutions:.....	274
Chapter 32 Solutions:.....	276
Chapter 33 Solutions:.....	277
Chapter 34 Solutions:.....	280
Chapter 35 Solutions:.....	283
Chapter 36 Solutions:.....	284
Chapter 37 Solutions:.....	287
Chapter 38 Solutions:.....	291
Chapter 39 Solutions:.....	292
GNU Free Documentation License.....	294
B.1 PREAMBLE.....	294

Introduction

Discrete math has become increasingly important in recent years, for a number of reasons: *The Art of Problem Solving* <http://www.artofproblemsolving.com/articles/discrete-math>

Discrete math is essential to college-level mathematics and beyond.

Discrete math — together with calculus and abstract algebra — is one of the core components of mathematics at the undergraduate level. Students who learn a significant quantity of discrete math before entering college will be at a significant advantage when taking undergraduate-level math courses.

Discrete math is the mathematics of computing.

The mathematics of modern computer science is built almost entirely on discrete math, in particular combinatorics and graph theory. This means that in order to learn the fundamental algorithms used by computer programmers, students will need a solid background in these subjects. Indeed, at most universities, an undergraduate-level course in discrete mathematics is a required part of pursuing a computer science degree.

Discrete math is very much “real world” mathematics.

The mathematics of modern computer science is built almost entirely on discrete math, in particular combinatorics and graph theory. This means that in order to learn the fundamental algorithms used by computer programmers, students will need a solid background in these subjects. Indeed, at most universities, an undergraduate-level course in discrete mathematics is a required part of pursuing a computer science degree.

Discrete math shows up on most middle and high school math contests.

Prominent math competitions such as MATHCOUNTS (at the middle school level) and the American Mathematics Competitions (at the high school level) feature discrete math questions as a significant portion of their contests. On harder high school contests, such as the AIME, the quantity of discrete math is even larger. Students that do not have a discrete math background will be at a significant disadvantage in these contests. In fact, one prominent MATHCOUNTS coach tells us that he spends nearly 50% of his preparation time with his students covering counting and probability topics, because of their importance in MATHCOUNTS contests.

Discrete math teaches mathematical reasoning and proof techniques.

Algebra is often taught as a series of formulas and algorithms for students to memorize (for example, the quadratic formula, solving systems of linear equations by substitution, etc.), and geometry is often taught as a series of “definition-theorem-proof” exercises that are often done by rote (for example, the infamous “two-column proof”). While

undoubtedly the subject matter being taught is important, the material (as least at the introductory level) does not lend itself to a great deal of creative mathematical thinking. By contrast, with discrete mathematics, students will be thinking flexibly and creatively right out of the box. There are relatively few formulas to memorize; rather, there are a number of fundamental concepts to be mastered and applied in many different ways.

Discrete math is fun!

Many students, especially bright and motivated students, find algebra, geometry, and even calculus dull and uninspiring. Rarely is this the case with most discrete math topics. When we ask students what their favorite topic is, most respond either "combinatorics" or "number theory." (When we ask them what their least favorite topic is, the overwhelming response is "geometry.") Simply put, most students find discrete math more fun than algebra or geometry.

PART I: Logic, Sets, Proof

Chapter 1: Logical Connectives and Compound Propositions

The basic objects in logic are **propositions**. A proposition is a statement which is either true (T) or false (F) but not both. For example in the language of mathematics $p: 3 + 3 = 6$ is a true proposition while $q: 2 + 3 = 6$ is a false proposition. *What do you want for lunch?* is a question, not a proposition. Likewise *Get lost!* is a command, not a proposition. The sentence *There are exactly $10^{87} + 3$ stars in the universe* is a proposition, despite the fact that no one knows its truth value. Here are two, more subtle, examples:

- (1) *He is more than three feet tall* is not a proposition since, until we are told to whom *he* refers, the statement cannot be assigned a truth value. The mathematical sentence $x + 3 = 7$ is not a proposition for the same reason. In general, sentences containing variables are not propositions unless some information is supplied about the variables. More about that later however.
- (2) *This sentence is false* is not a proposition. It seems to be both true and false. In fact if it is T then it says it is F and if it is F then it says it is T. It can be dangerous using sentences that refer to themselves. Of course, using a knife can also be dangerous, but we do use knives safely when we are careful. Likewise, using self-referential sentences can be done safely if care is taken.

Sometimes a little common sense is required. For example, *It is raining* is a proposition, but its truth value is not constant and may be arguable. That is, someone might say *It is not raining, it is just drizzling*, or *Do you mean on Venus?* Feel free to ignore this sort of quibbling.

Simple propositions, such as *It is raining*, and *The streets are wet*, can be combined to create more complicated propositions such as *It is raining and the streets are not wet*. These sorts of involved propositions are called **compound propositions**. Compound propositions are built up from simple propositions using a number of **connectives** to join or modify the simple propositions. In the last example, the connectives are **and** which joins the two clauses, and **not**, which modifies the second clause.

It is important to keep in mind that since a compound proposition is, after all, a proposition, it must be classifiable as either true or false. That is, it must be possible to assign a truth value to any compound proposition. There are mutually agreed upon rules to allow the determination of exactly when a compound proposition is true and when it is false. Luckily these rules jibe nicely with common sense (with one small exception), so they are easy to remember and understand.

The simplest logical connective is **negation**. In normal English sentences, this connective is indicated by appropriately inserting *not* in the statement, by preceding the statement with *it is not the case that*, or for mathematical statements, by using a slanted slash. For example, if p is the

proposition $2 + 3 = 4$, then the negation of p is denoted by the symbol $\neg p$ and it is the proposition $2 + 3 \neq 4$. In this case, p is false and $\neg p$ is true. If p is *It is raining*, then $\neg p$ is *It is not raining* or even the stilted sounding *It is not the case that it is raining*. The negation of a proposition p is the proposition whose truth value is the opposite of p in all cases. The behavior of $\neg p$ can be exhibited in a **truth table**. In each row of the truth table 1.1 we list a possible truth value of p and the corresponding truth value of $\neg p$.

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

Table 1.1: Logical Negation

The connective that corresponds to the word *and* is called **conjunction**. The conjunction of p with q is denoted by $p \wedge q$ and read as *p and q*. The conjunction of p with q is declared to be true exactly when both of p, q are true. It is false otherwise. This behavior is exhibited in the truth table 1.2.

Four rows are required in this table since when p is true, q may be either true or false and when p is false it is possible for q to be either true or false. Since a truth value must be assigned to $p \wedge q$ in every possible case, one row in the truth table is needed for each of the four possibilities.

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

Table 1.2: Logical And

The logical connective **disjunction** corresponds to the word *or* of ordinary language. The disjunction of p with q is denoted by $p \vee q$, and read as *p or q*. The disjunction $p \vee q$ is true if at least one of p, q is true.

Disjunction is also called **inclusive-or**, since it includes the possibility that both component statements are true. In everyday language, there is a second use of *or* with a different meaning. For example, in the proposition *Your ticket wins a prize if its serial number contains a 3 or a 5*, the *or* would normally be interpreted in the inclusive sense (tickets that have both a 3 and 5 are still winners), but in the proposition *With dinner you get mashed potatoes or french fries*, the *or* is being used in the **exclusive-or** sense.

The exclusive-or is also called the **disjoint disjunction** of p with q and is denoted by $p \oplus q$. Read that as *p xor q* if it is necessary to say it in words. The value of $p \oplus q$ is true if exactly one of p, q is true. The exclusion of both being true is the difference between inclusive-or and exclusive-or. The truth table shown officially defines these two connectives. In a mathematical setting one usually assumes the inclusive-or is intended unless the exclusive sense is explicitly indicated.

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

Table 1.3: Logical or and Logical xor

The next two logical connectives correspond to the phrases *If $\dots$, then $\dots$* and the (rarely used in real life but common in math) *$\dots$ if and only if $\dots$* . In mathematical discussions, ordinary English words are used in ways that usually correspond to the way we use words in normal conversation. The connectives **not**, **and**, **or** mean pretty much what would be expected. But the **implication**, denoted $p \rightarrow q$ and read as *If p , then q* can be more subtle. This is partly because when the *If p , then q* construction is used in everyday speech, there is an implied connection between the proposition p (called the **hypothesis**) and the proposition q (called the **conclusion**). For example, in the statement *If I study, then I will pass the test*, there is an assumed connection between studying and passing the test. However, in logic, the connective is going to be used to join any two propositions, with no relation necessary between the hypothesis and conclusion. What truth value should be assigned to such bizarre sentences as *If I study, then the moon is 238,000 miles from earth?*

p	q	p	$\rightarrow$	q
T	T	T	T	T
T	F	T	F	F
F	T	F	T	T
F	F	F	T	F

Table 1.4: Logical Implication

Is it true or false? Or maybe it is neither one? Well, that last option isn't too pleasant because that sentence is supposed to be a proposition, and to be a proposition it has to have truth value either T or F. So it is going to have to be classified as one or the other. In everyday conversation, the choice isn't likely to be too important whether it is classified it as either true or false in the case described. But an important part of mathematics is knowing when propositions are true and when they are false. The official choices are given in the truth table for $p \rightarrow q$. We can make sense of this with an example.

Example 1.1. First consider the statement which Bill's dad makes to Bill: *If you get an A in math, then I will buy you a new car.* If Bill gets an A and his dad buys him a car, then dad's statement is true, and everyone is happy (that is the first row in the table). In the second row, Bill gets an A, and his dad doesn't come through. Then Bill's going to be rightfully upset since his father lied to him (dad made a false statement). In the last row of the table he can't complain if he doesn't get an A, and his dad doesn't buy him the car (so again dad made a true statement). Most people feel comfortable with those three rows. In the third row of the table, Bill doesn't get an A, and his dad buys him a car anyhow. This is the funny case. It seems that calling dad a liar in this case would be a little harsh on the old man. So it is declared that dad

told the truth. Remember it this way: an implication is true unless the hypothesis is true and the conclusion is false.

The **biconditional** is the logical connective corresponding to the phrase $\dots$ if and only if $\dots$. It is denoted by $p \Leftrightarrow q$, (read p if and only if q), and often more tersely written as p iff q . The biconditional is true when the two component propositions have the same truth value, and it is false when their truth values are different. Examine the truth table to see how this works.

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

Table 1.5: Logical biconditional

The connectives described above combine at most two simple propositions. More complicated propositions can be formed by joining compound propositions with those connectives. For example, $p \wedge (\neg q)$, $(p \vee q) \rightarrow (q \wedge (\neg r))$, and $(p \rightarrow q) \Leftrightarrow ((\neg p) \vee q)$ are compound propositions, where parentheses have been used, just as in ordinary algebra, to avoid ambiguity. Such extended compound propositions really are propositions. That is, if the truth value of each component is known, it is possible to determine the truth value of the entire proposition. The necessary computations can be exhibited in a truth table.

Example 1.2. Let p, q and r be propositions. To construct a truth table for $(p \wedge q) \rightarrow r$, first notice that eight rows will be needed in the table to account for all the possible combinations of truth values of the simple component statements p, q and r . This is so since there are, as noted above, four rows needed to account for the choices for p and q , so there will be those four rows paired with r having truth value T, and four more with r having truth value F, for a total of $4 + 4 = 8$. In general, if there are n simple propositions in a compound statement, the truth table for the compound statement will have 2^n rows. The truth table for $(p \wedge q) \rightarrow r$ is given in Table 1.6, with an auxiliary column for $p \wedge q$ to serve as an aid for filling in the last column.

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

Table 1.6: Truth Table for $(p \wedge q) \rightarrow r$

Be careful about how propositions are grouped. For example, if truth tables for $p \wedge (q \rightarrow r)$ and

$(p \wedge q) \rightarrow r$ are constructed, they turn out not to be the same in every row. Specifically, if p is false, then $p \wedge q$ is false, and $(p \wedge q) \rightarrow r$ is true. Whereas when p is false $p \wedge (q \rightarrow r)$ is false. So writing $p \wedge q \rightarrow r$ is ambiguous.

Here are a few examples of translating between propositions expressed in ordinary language and propositions expressed in the language of logic.

Example 1.3. Let c be the proposition *It is cold* and s : *It is snowing*, and h : *I'm staying home*. Then $(c \wedge s) \rightarrow h$ is the proposition *If it is cold and snowing, then I'm staying home*. While $(c \vee s) \rightarrow h$ is *If it is either cold or snowing, then I'm staying home*. Messier is $\neg(h \rightarrow c)$ which can be expressed as *It is not the case that if I stay home, then it is cold*, which is a little too convoluted. Translating in the other direction, the proposition *It is snowing and it is either cold or I'm staying home* would be symbolized as $s \wedge (c \vee h)$. Notice the parentheses are needed in this last proposition since $(s \wedge c) \vee h$ does not capture the meaning of the ordinary language sentence, and $s \wedge c \vee h$ is ambiguous.

There is a connection between logical connectives and certain operations on bit strings. There are two **binary digits** (or **bits**): 0 and 1. A **bit string of length n** is any sequence of n bits. For example, 0010 is a bit string of length four. Computers use bit strings to encode and manipulate information. Some bit string operations are really just disguised truth tables. Here is the connection: Since a bit can be one of two values, bits can be used to represent truth values. Let T correspond to 1, and F to 0. Then given two bits, logical connectives can be used to produce a new bit. For example $\neg 1 = 0$, and $1 \vee 1 = 1$. This can be extended to strings of bits of the same length by combining corresponding bit in the two strings. For example,

$$01011 \wedge 11010 = (0 \wedge 1)(1 \wedge 1)(0 \wedge 0)(1 \wedge 1)(1 \wedge 0) = 01010.$$

Exercises

Exercise 1.1. Determine which of the following sentences are propositions. Assume you are speaking the sentence.

- a) *There are seven days in a week.*
- b) *Get lost!*
- c) *Pistachio is the best ice cream flavor.*
- d) *All unicorns had four legs.*

Exercise 1.2. Construct truth tables for each of the following.

- a) $p \oplus \neg q$
- b) $\neg(q \rightarrow p)$
- c) $q \wedge \neg p$
- d) $\neg q \vee p$
- e) $p \rightarrow (\neg q \wedge r)$

Exercise 1.3. Perform the indicated bit string operations. The bit strings are given in groups of four bits each for ease of reading.

- a) $(1101\ 0111 \oplus 1100\ 0010) \wedge 1100\ 1000$
- b) $(1111\ 1010 \wedge 0111\ 0010) \vee 0101\ 0001$
- c) $(1001\ 0010 \vee 0101\ 1101) \wedge (0110\ 0010 \vee 0111\ 0101)$

Exercise 1.4. Let s be the proposition “*It is snowing.*” and f be the proposition “*It is below freezing.*”. Convert the following English sentences into statements using the symbols s , f and logical connectives.

- a) *It is snowing and it is not below freezing.*
- b) *It is below freezing and it is not snowing.*
- c) *If it is not snowing, then it is not below freezing.*

Exercise 1.5. Let j be the proposition “*Jordan played.*” and b be the proposition “*The Bulls won.*”. Write the following statements as English sentences.

- a) $\neg j \wedge b$
- b) $j \rightarrow \neg b$
- c) $b \vee j$
- d) $b \rightarrow \neg j$

Exercise 1.6. Let c be the proposition “*Sam plays chess.*” and b be the proposition “*Sam has the black pieces.*” and w be the proposition “*Sam wins.*”.

- a) Translate into English: $(c \wedge \neg b) \rightarrow w$.
- b) Translate into symbols: *If Sam didn’t win her chess game, then she played black.*

Problems

Problem 1.1. Determine which of the following sentences are propositions. Assume you are speaking the sentence.

- a) *Today is Tuesday.*
- b) *Why are you whining?*
- c) *The Vikings are the worst team in professional sports.*
- d) *This sentence has five words.*
- e) *There is a black hole at the center of every galaxy.*

Problem 1.2. Construct truth tables for each of the following.

- a) $\neg q \rightarrow \neg p$.
- b) $p \rightarrow (q \wedge r)$. (You will need eight rows for this one.)

Problem 1.3. Perform the indicated bit string operations. The bit strings are given in groups of four bits each for ease of reading.

- a) $(1001\ 0101 \oplus 1010\ 0110) \wedge 1100\ 1000$
- b) $(1110\ 1010 \wedge 0101\ 0010) \vee 0111\ 1001$
- c) $(1111\ 0011 \vee 0111\ 0101) \wedge (0010\ 0010 \vee 0110\ 0100)$

Problem 1.4. Let s be the proposition “*It is snowing.*” and f be the proposition “*It is below freezing.*”. Convert the following English sentences into statements using the symbols s, f and logical connectives.

- a) *It is snowing and it not below freezing.*
- b) *It is snowing, then it is below freezing.*

Chapter 2: Logical Equivalence

It is clear that the propositions *It is sunny and it is warm* and *It is warm and it is sunny* mean the same thing. More generally, for any propositions p, q , we see that $p \wedge q$ and $q \wedge p$ have the same meaning. To say it a little differently, for any choice of truth values for p and q , the propositions $p \wedge q$ and $q \wedge p$ have the same truth value. One more time: $p \wedge q$ and $q \wedge p$ have identical truth tables.

Two propositions with identical truth values are called logically equivalent. The expression $p \equiv q$ means p and q are logically equivalent.

Some logical equivalences are not as transparent as the example above. With a little thought it should be clear that *I am not taking math or I am not taking physics* means the same as *It's not the case that I am taking math and physics*. In symbols, $(\neg m) \vee (\neg p)$ means the same as $\neg(m \wedge p)$.

Example 2.1 (De Morgan). *Prove that $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ using a truth table. We construct the truth table 2.1 in the order of precedence: $\neg$ before $\wedge$ or $\vee$, but the expression in parentheses has highest precedence. We construct the table using additional columns for compound parts of the two expressions.*

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

Table 2.1: De Morgan's Law

It may be a little harder to believe $(p \rightarrow q) \equiv (\neg p \vee q)$, but checking a truth table shows they are in fact equivalent. Saying *If it is Monday, then I am tired* is identical to saying *It isn't Monday or I am tired*. You should construct a truth table to demonstrate their equivalence.

A proposition, $\mathbb{T}$, which is always true is called a **tautology**. A **contradiction** is a proposition, $\mathbb{F}$, which is always false. The prototype example of a tautology is $p \vee \neg p$, and for a contradiction, $p \wedge \neg p$. Notice that since $p \Leftrightarrow q$ is T exactly when p and q have the same truth value, two propositions p and q will be logically equivalent provided $p \Leftrightarrow q$ is a tautology.

Table 2.2 contains the most often used logical equivalences. These are well worth learning by sight and by name.

Equivalence	Name
$\neg(\neg p) \equiv p$	Double Negation
$p \wedge \mathbb{T} \equiv p$	Tautology Identity
$p \vee \mathbb{F} \equiv p$	Contradiction Identity
$p \vee \mathbb{T} \equiv \mathbb{T}$	Tautology Domination
$p \wedge \mathbb{F} \equiv \mathbb{F}$	Contradiction Domination
$p \vee p \equiv p$	Disjunctive Idempotent law
$p \wedge p \equiv p$	Conjunctive Idempotent law
$p \vee q \equiv q \vee p$	Disjunction Commutative law
$p \wedge q \equiv q \wedge p$	Conjunction Commutative law
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Disjunction Associative law
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Conjunction Associative law
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Disjunctive Distributive law
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Conjunctive Distributive law
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan's law for Conjunction
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's law for Disjunction
$p \vee \neg p \equiv \mathbb{T}$	Law of Excluded Middle
$p \wedge \neg p \equiv \mathbb{F}$	Law of Contradiction
$p \rightarrow q \equiv \neg p \vee q$	Disjunctive or form
$p \rightarrow q \equiv \neg q \rightarrow \neg p$	Implication $\equiv$ Contrapositive
$\neg p \rightarrow \neg q \equiv q \rightarrow p$	Inverse $\equiv$ Converse

Table 2: Logical Equivalences

There are three propositions related to the basic **If ..., then ...** implication: $p \rightarrow q$. First $\neg q \rightarrow \neg p$ is called the **contrapositive** of the implication. The **converse** of the implication is the proposition $q \rightarrow p$. Finally, the **inverse** of the implication is $\neg p \rightarrow \neg q$. Using a truth table, it is easy to check that an implication and its contrapositive are logically equivalent, as are the converse and the inverse. A common slip is to think the implication and its converse are logically equivalent. Checking a truth table shows that isn't so. The implication *If an integer ends with a 2, then it is even* is T, but its converse, *If an integer is even, then it ends with a 2*, is certainly F.

Five basic connectives have been given: $\neg, \wedge, \vee, \rightarrow, \Leftrightarrow$, but that is really just for convenience. It is possible to eliminate some of them using logical equivalences. For example, $p \Leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ so there really is no need to explicitly use the biconditional. Likewise, $p \rightarrow q \equiv \neg p \vee q$, so the use of the implication can also be avoided. Finally, $p \wedge q \equiv \neg(\neg p \vee \neg q)$ so that there really is no need ever to use the connective $\wedge$. Every proposition made up of the five basic connectives can be rewritten using only $\neg$ and $\vee$ (probably with a great loss of clarity however).

The most often used standardization, or normalization, of logical propositions is the **disjunctive normal form (DNF)**, using only $\neg$ (negation), $\wedge$ (conjunction), and $\vee$ (disjunction). A propositional form is considered to be in DNF if and only if it is a disjunction of one or more conjunctions of one or more *literals* (a *literal* is a letter or a letter preceded by the negation symbol).

For example, the following are all in disjunctive normal form:

- $p \wedge q$
- p
- $(a \wedge q) \vee r$
- $(p \wedge \neg q \wedge \neg r) \vee (\neg s \wedge t \wedge u)$

While these are not in DNF:

- $\neg(p \vee q)$ – since it is not the disjunction of literals.
- $p \wedge (q \wedge (r \vee s))$ – since an or is embedded in a conjunction.

It is always possible to verify a logical equivalence via a truth table. But it is also possible to verify equivalences by stringing together previously known equivalences. We provide two examples of this process.

Example 2.2. Show $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$. The plan is to start with the expression $\neg(p \vee (\neg p \wedge q))$, work through a sequence of equivalences ending up with $\neg p \wedge \neg q$. It's pretty much like proving identities in algebra or trigonometry.

$$\begin{array}{ll}
 \text{Proof.} & \neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg(\neg p \wedge q) && \text{De Morgan's Law} \\
 & \equiv \neg p \wedge (\neg(\neg p) \vee \neg q) && \text{De Morgan's Law} \\
 & \equiv \neg p \wedge (p \vee \neg q) && \text{Double Negation Law} \\
 & \equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{Distributive Law} \\
 & \equiv (p \wedge \neg p) \vee (\neg p \wedge \neg q) && \text{Commutative Law} \\
 & \equiv \mathbb{F} \vee (\neg p \wedge \neg q) && \text{Law of Contradiction} \\
 & \equiv (\neg p \wedge \neg q) \vee \mathbb{F} && \text{Commutative Law} \\
 & \equiv (\neg p \wedge \neg q) && \text{Identity Law} \blacksquare
 \end{array}$$

Example 2.3. Show $(p \wedge q) \rightarrow (p \vee q) \equiv \mathbb{T}$.

$$\begin{array}{ll}
 \text{Proof.} & (p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q) && \text{Disjunctive or form} \\
 & \equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{De Morgan's Law} \\
 & \equiv \neg p \vee (\neg q \vee p) \vee q && \text{Associative Law} \\
 & \equiv \neg p \vee (p \vee \neg q) \vee q && \text{Commutative Law} \\
 & \equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{Associative Law} \\
 & \equiv \mathbb{T} \vee \mathbb{T} && \text{Excluded Middle} \\
 & \equiv \mathbb{T} && \text{Identity Law} \blacksquare
 \end{array}$$

Exercises

Exercise 2.1. Use truth tables to verify each of the following equivalences:

- a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$
- b) $\neg p \wedge (p \vee q) \equiv \neg(q \rightarrow p)$
- c) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \wedge r)$

Exercise 2.2. Show that the statements are not logically equivalent (find a specific counterexample):

- a) $p \wedge (q \rightarrow r) \not\equiv (p \wedge q) \rightarrow r$
- b) $p \rightarrow q \not\equiv q \rightarrow p$
- c) $p \rightarrow q \not\equiv \neg p \rightarrow \neg q$

Exercise 2.3. Use truth tables to show that the following are tautologies:

- a) $[p \wedge (p \rightarrow q)] \rightarrow q$
- b) $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$

Exercise 2.4. Consider the implication “If it is Saturday, then I will mow the lawn.”.

- a) Write the converse of the implication.
- b) Write the inverse of the implication.
- c) Write the contrapositive of the implication.

Exercise 2.5. Consider the three answers to exercise 2.4. One of the three is logically equivalent to the implication. Which one? Two of the three are not logically equivalent to the implication, but are logically equivalent to each other. Which two?

Exercise 2.6. The statements below are not tautologies. In each case, find an assignment of truth values to the literals, (that is, a letter or a letter preceded by a negation symbol) so the statement is false.

- a) $[(p \wedge q) \rightarrow r] \leftrightarrow [(p \rightarrow r) \wedge (q \rightarrow r)]$
- b) $[(p \wedge q) \vee r] \rightarrow [p \wedge (q \vee r)]$

Exercise 2.7. Give a proof of $(p \wedge \neg r) \rightarrow \neg q \equiv p \rightarrow (q \rightarrow r)$ using the Fundamental Logical Equivalences, following the pattern of examples 2.2 and 2.3.

Problems

Problem 2.1. Use a truth table to show $p \rightarrow q \equiv \neg p \vee q$.

Problem 2.2. Use a truth table to show $(p \wedge q) \rightarrow r \equiv p \rightarrow (q \rightarrow r)$.

Problem 2.3. Use a truth table to show that $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

Problem 2.4. Consider the implication “If I work, then I get paid.”:

- Write the converse of the implication.
- Write the inverse of the implication.
- Write the contrapositive of the implication.
- Write the inverse of the contrapositive of the implication.

Problem 2.5. Consider the four answers for problem 2.4. Which of them are logically equivalent to the implication? Which of the four are not logically equivalent to the implication, (but are logically equivalent to each other)?

Problem 2.6. Use a truth table to show that $[p \rightarrow (q \rightarrow r)] \not\equiv [(p \rightarrow q) \rightarrow r]$.

Problem 2.7. Use truth tables to show that the following are tautologies.

- $(p \wedge q) \rightarrow p$
- $[(p \vee q) \rightarrow r] \rightarrow [(p \rightarrow r) \wedge (q \rightarrow r)]$

Problem 2.8. Give a proof of $\neg p \rightarrow (p \rightarrow q) \equiv \mathbb{T}$ using the Fundamental Logical Equivalences, following the pattern of examples 2.2 and 2.3.

Chapter 3: Predicates and Quantifiers

The sentence $x^2 - 2 = 0$ is not a proposition. It cannot be assigned a truth value unless some more information is supplied about the variable x . Such a statement is called a **predicate** or a **propositional function**.

Instead of using a single letter to denote a predicate, a symbol such as $S(x)$ will be used to indicate the dependence of the sentence on a variable. Here are two more examples of predicates.

- (1) $A(c)$: *Al drives a c*, and
- (2) $B(x, y)$: *x is the brother of y*.

The second example is an instance of a **two-place predicate**.

With a given predicate, there is an associated set of objects which can be used in place of the variables. For example, in the predicate $S(x)$: $x^2 - 2 = 0$, it is understood that the x can be replaced by a number. Replacing x by, say, the word *blue* does not yield a meaningful sentence. For the predicate $A(c)$ above, c can be replaced by, say, makes of cars (or maybe types of nails!). For $B(x, y)$, the x can be replaced by any human male, and the y by any human. The collection of possible replacements for a variable in a predicate is called the **domain of discourse** for that variable. Usually, the domain of discourse is left for the reader to guess, but if the domain of discourse is something other than an obvious choice, the writer will mention the domain to be used.

A predicate is not a proposition, but it can be converted into a proposition. There are three ways to modify a predicate to change it into a proposition. Let's use $S(x)$: $x^2 - 2 = 0$ as an example.

The first way to change $S(x)$ to make it into a proposition is to assign a specific value from the variable's domain of discourse to the variable. For example, setting $x = 3$, gives the (false) proposition $S(3)$: $3^2 - 2 = 0$. On the other hand, setting $x = \sqrt{2}$ gives the (true) proposition $S(\sqrt{2})$: $(\sqrt{2})^2 - 2 = 0$. The process of setting a variable equal to a specific object in its domain of discourse is called **instantiation**. Looking at the two-place predicate $B(x, y)$: *x is the brother of y*, we can instantiate both variables to get the (true - look up the Osmonds) proposition $B(\text{Donny}, \text{Marie})$: *Donny is the brother of Marie*. Notice that the sentence $B(\text{Donny}, y)$: *Donny is the brother of y* has not been converted into a proposition since it cannot be assigned a truth value without some information about y . But it has been converted from a two-place predicate to a one-place predicate.

A second way to convert a predicate to a proposition is to precede the predicate with the phrase *There is an x such that*. For example, *There is an x such that* $S(x)$ would become *There is an x*

such that $x^2 - 2 = 0$. This proposition is true if there is at least one choice of x in its domain of discourse for which the predicate becomes a true statement. The phrase *There is an x such that* is denoted in symbols by $\exists x$. The proposition above would be written $\exists x, S(x)$ or $\exists x(x^2 - 2 = 0)$. When trying to determine the truth value of the proposition $\exists x P(x)$, it is important to keep the domain of discourse for the variable in mind. For example, if the domain for x in $\exists x(x^2 - 2 = 0)$ is all integers, the proposition is false. But if its domain is all real numbers, the proposition is true. The phrase *There is an x such that* (or, in symbols, $\exists x$) is called **existential quantification**. In English it can also be read as *There exists x* or *For some x* .

The third and final way to convert a predicate into a proposition is by **universal quantification**. The phrase *For all x* is also rendered in English as *For each x* or *For every x* . The universal quantification of a predicate, $P(x)$, is obtained by preceding the predicate with the phrase *For all x* , producing the proposition *For all $x, P(x)$* , or, in symbols, $\forall x P(x)$. This proposition is true provided the predicate becomes a true proposition for every object in the variable's domain of discourse. Again, it is important to know the domain of discourse for the variable since the domain will have an effect on the truth value of the quantified proposition in general.

For multi-placed predicates, these three conversions can be mixed and matched. For example, using the obvious domains for the predicate $B(x, y)$: *x is the brother of y* here are some conversions into propositions:

- 1) $B(\text{Donny}, \text{Marie})$ has both variables instantiated. The proposition is true.
- 2) $\exists y B(\text{Donny}, y)$ is also a true proposition. It says *Donny* is somebody's brother. The first variable was instantiated, the second was existentially quantified.
- 3) $\forall y B(\text{Donny}, y)$ says everyone has *Donny* for a brother, and that is false.
- 4) $\forall x \exists y B(x, y)$ says that every male is somebody's brother and that is false.
- 5) $\exists y \forall x B(x, y)$ says there is a person for whom every male is a brother, and that is false.
- 6) $\forall x B(x, x)$ says every male is his own brother, and that is false.

Translation between ordinary language and symbolic language can get a little tricky when quantified statements are involved. Here are a few more examples.

Example 3.1. Let $P(x)$ be the predicate *x owns a Porsche*, and let $S(x)$ be the predicate *x speeds*. The domain of discourse for the variable in each predicate will be the collection of all drivers. The proposition $\exists x P(x)$ says **Someone owns a Porsche**. It could also be translated as **There is a person x such that x owns a Porsche**, but that sounds too stilted for ordinary conversation. A smooth translation is better. The proposition $\forall x(P(x) \rightarrow S(x))$ says **All Porsche owners speed**.

Translating in the other direction, the proposition *No speeder owns a Porsche* could be expressed as $\forall x(S(x) \rightarrow \neg P(x))$.

Example 3.2. Here's a more complicated example: translate the proposition **Al knows only Bill** into symbolic form. Let's use $K(x, y)$ for the predicate x **knows** y . The translation would be $K(Al, Bill) \wedge \forall x (K(Al, x) \rightarrow (x = Bill))$.

Example 3.3. For one last example, let's translate **The sum of two even integers is even** into symbolic form. Let $E(x)$ be the predicate x **is even**. As with many statements in ordinary language, the proposition is phrased in a shorthand code that the reader is expected to unravel. As given, the statement doesn't seem to have any quantifiers, but they are implied. Before converting it to symbolic form, it might help to expand it to its more long-winded version: **For every choice of two integers, if they are both even, then their sum is even**. Expressed this way, the translation to symbolic form is: $\forall x \forall y ((E(x) \wedge E(y)) \rightarrow E(x + y))$.

Notice that if the domain of discourse consists of finitely many entries $a_1, \dots, a_n$, then

$$\forall x p(x) \equiv p(a_1) \vee p(a_2) \vee \dots \vee p(a_n).$$

So the quantifier $\forall$ can be expressed in terms of the logical connective $\wedge$. The existential quantifier and $\vee$ are similarly linked: $\exists x p(x) \equiv p(a_1) \vee p(a_2) \vee \dots \vee p(a_n)$.

From the associative and commutative laws of logic we see that we can rearrange any system of propositions which are linked only by $\wedge$'s or linked only by $\vee$'s. For instance, consider the previous examples 3.1 – 3.3 with finite domains of discourse. Consequently, any more generally quantified proposition of the form $\forall x \forall y p(x, y)$ is logically equivalent to $\forall y \forall x p(x, y)$. Similarly for statements which contain only existential quantifiers. But the distributive laws come into play when $\wedge$'s and $\vee$'s are mixed. So, care must be taken with predicates which contain both existential and universal quantifiers, as the following example shows.

Example 3.4. Let $p(x, y): x + y = 0$ and let the domain of discourse be all real numbers for both x and y . The proposition $\forall y \exists x p(x, y)$ is true: given y , by setting (instantiating) $x = -y$ we convert $x + y = 0$ to the true statement $(-y) + y = 0$. In fact, $(\forall y \in \mathbb{R})[(-y) + y = 0]$ is a tautology. However the proposition $\exists x \forall y p(x, y)$ is false. If we set (instantiate) $y = 1$, then $x + y = 0$ implies $x = -1$. When we set $y = 0$, we get $x = 0$. Since $0 \neq -1$ there is no x which will work for all y , since it would have to work for the specific values of $y = 0$ and $y = 1$.

To form the negation of quantified statements, we apply De Morgan's laws. This can be seen in case of a finite domain of discourse as follows:

$$\begin{aligned} \neg(\forall x p(x)) &\equiv \neg(p(a_1) \wedge p(a_2) \wedge \dots \wedge p(a_n)) \\ &\equiv \neg p(a_1) \vee \neg p(a_2) \vee \dots \vee \neg p(a_n) \\ &\equiv \exists x \neg p(x) \end{aligned}$$

In the same way, we have $\neg(\exists x p(x)) \equiv (\forall x \neg p(x))$.

Exercises

Exercise 3.1. Let $p(x): 2x \geq 4$, for integers x . Determine the truth values of the following propositions.

- a) $p(2)$
- b) $p(-3)$
- c) $\forall x [(x \leq 10) \rightarrow p(x)]$
- d) $\exists x \neg p(x)$

Exercise 3.2. Let $p(x, y)$ be x has read y , where the domain of discourse for x is all students in this class, and the domain of discourse for y is all novels. Express the following propositions in English.

- a) $\forall x p(x, \text{War and Peace})$
- b) $\exists x \neg p(x, \text{The Great Gatsby})$
- c) $\exists x \forall y p(x, y)$
- d) $\forall y \exists x p(x, y)$

Exercise 3.3. Let $E(x, y)$ be the statement x can fool y , where the domain of discourse for both x and y is all people. Use quantifiers to express each of the following statements.

- a) *I can fool everyone.*
- b) *George can't fool anybody.*
- c) *No one can fool himself.*
- d) *There is someone who can fool everybody.*
- e) *There is someone everyone can fool.*
- f) *Ralph can fool two different people.*

Exercise 3.4. Negate each of the statements from exercise 3.2 in English.

Exercise 3.5. Negate each statement from exercise 3.3 in logical symbols. Of course, the easy answer would be to simply put $\neg$ in front of each statement. But use the principle given at the end of this chapter to move the negation across the quantifiers.

Exercise 3.6. Express symbolically: The product of an even integer and an odd integer is even.

Exercise 3.7. Express in words the meaning of

$$\exists x P(x) \wedge \forall x \forall y ((P(x) \wedge P(y)) \rightarrow (x = y)).$$

Problems

Problem 3.1. Let h be Ben is healthy., w : Ben is wealthy., and s : Ben is wise. Express the following in English:

- a) $h \wedge w$
- b) $w \vee s$
- c) $h \rightarrow (w \wedge s)$
- d) $(h \rightarrow w) \wedge s$

Problem 3.2. Let $S(x, y)$ be the predicate x has seen y where the domain of discourse for x is all students in this class and the domain of discourse for y is all movies. Express the following in logical symbols using quantifiers.

- a) Every student in this class has seen *The Avengers*.
- b) No student in this class has seen *Life of Pi*.
- c) *Hidden Figures* has been seen by someone in this class.
- d) Some students have seen every movie.
- e) For each movie, there is at least one student in the class who has seen that movie.

Problem 3.3. Negate the propositions in problem 3.1 in English.

Problem 3.4. Negate the propositions in problem 3.2 in symbols. Note: An easy way to do this is to simply write $\neg$ in front of the answers in problem 3.2. Don't do that! Give the negation with no quantifiers coming after the negation symbol.

Problem 3.5. Negate the propositions in problem 3.2 in English. Note: An easy way to do this is to simply write "It is not the case that" in front each proposition. Don't do that! Give the negation as a reasonably natural English sentence.

Chapter 4: Rules of Inference

The heart of mathematics is proof. In this chapter, we give a careful description of what exactly constitutes a proof in the realm of propositional logic. Throughout the course various methods of proof will be demonstrated, including the particularly important style of proof called *induction*. It's important to keep in mind that all proofs, no matter what the subject matter might be, are based on the notion of a valid argument as described in this chapter, so the ideas presented here are fundamental to all of mathematics.

Imagine trying carefully to define what a proof is, and it quickly becomes clear just how difficult a task that is. So it shouldn't come as a surprise that the description takes on a somewhat technical looking aspect. But don't let all the symbols and abstract-looking notation be misleading. All these rules really boil down to plain old common sense when looked at correctly.

The usual form of a theorem in mathematics is: If a is true and b is true and c is true, etc., then s is true. The $a, b, c, \dots$ are called the **hypotheses**, and the statement s is called the **conclusion**. For example, a mathematical theorem might be: if m is an even integer and n is an odd integer, then mn is an even integer. Here the hypotheses are m is an even integer and n is an odd integer, and the conclusion is mn is an even integer.

We begin by concerning ourselves with proofs from the realm of propositional logic rather than the sort of theorem mentioned above. We will be interested in arguments in which the **form** of the argument is the item of interest rather than the **content** of the statements in the argument.

For example, consider the simple argument: (1) *My car is either red or blue* and (2) *My car is not red*, and so (3) *My car is blue*. Here the hypotheses are (1) and (2), and the conclusion is (3). It should be clear that this is a **valid argument**. That means that if you agree that (1) and (2) are true, then you *must* accept that (3) is true as well.

Definition 4.1. An argument is called **valid** provided that if you agree that all the hypotheses are true, then you must accept the truth of the conclusion.

Now the content of that argument (in other words, the stuff about *my* and *cars* and *colors*) really have nothing to do with the validity of the argument. It is the **form** of the argument that makes it valid. The form of this argument is (1) $p \vee q$ and (2) $\neg p$, therefore (3) q . Any argument that has this form is valid, whether it talks about cars and colors or any other notions. For example, here is another argument of the very same form: (1) *I either read the book or just looked at the pictures* and (2) *I didn't read the book*, therefore (3) *I just looked at the pictures*.

Some arguments involve quantifiers. For instance, consider the classic example of a logical argument: (1) *All men are mortal* and (2) *Socrates is a man*, and so (3) *Socrates is mortal*. Here the hypotheses are the statements (1) and (2), and the conclusion is statement (3). If we let $M(x)$ be x is a man and $D(x)$ be x is mortal (with domain for x being everything!), then this argument could be symbolized as shown.

$$\begin{array}{l} \forall x(M(x) \rightarrow D(x)) \\ \underline{M(\text{Socrates})} \\ \hline \therefore D(\text{Socrates}) \end{array}$$

The general form of a proof that a logical argument is valid consists in assuming all the hypotheses have truth value T, and showing, by applying rules of logic, that the conclusion must also have truth value T.

Just what are the valid rules of logic that can be used in the course of the proof? They are called the Rules of Inference, and there are seven of them listed in table 4.1. Each rule of inference arises from a tautology, and actually there is no end to the rules of inference, since each new tautology can be used to provide a new rule of inference. But, in real life, people rely on only a few basic rules of inference, and the list provided in the table is plenty for all normal purposes.

It is important not to merely look on these rules as marks on the page, but rather to understand what each one says in words. For example, Modus Ponens corresponds to the common sense rule: if we are told *p is true*, and also *If p is true, then so is q*, then we would leap to the reasonable conclusion that *q is true*. That is all Modus Ponens says. Similarly, for the rule of proof of Disjunctive Syllogism: knowing *Either p or q is true*, and *p is not true*, we would immediately conclude *q is true*. That's the rule we applied in the *car* example above. Translate the remaining six rules of inference into such common sense statements. Some may sound a little awkward, but they ought to all elicit an *of course that's right* feeling once understood. Without such an understanding, the rules seem like a jumble of mystical symbols, and building logical arguments will be pretty difficult.

Name	Rule of Inference	
Modus Ponens	p and $p \rightarrow q$	$\therefore q$
Modus Tollens	$\neg q$ and $p \rightarrow q$	$\therefore \neg p$
Hypothetical Syllogism	$p \rightarrow q$ and $q \rightarrow r$	$\therefore p \rightarrow r$
Addition	p	$\therefore p \vee q$
Simplification	$p \wedge q$	$\therefore p$
Conjunction	p and q	$\therefore p \wedge q$
Disjunctive Syllogism	$p \vee q$ and $\neg p$	$\therefore q$

Table 4.1: Basic Rules of Inference

What exactly goes into a logical argument? Suppose we want to prove (or show valid) an argument of the form *If a and b and c are true, then so is s*. One way that will always do the trick is to construct a truth table as in examples earlier in the course. We check the rows in the table where all the hypotheses are true, and make sure the conclusion is also true in those rows. That would complete the proof. In fact that is exactly the method used to justify the seven rules

of inference given in the table. But building truth tables is certainly tedious business, and it certainly doesn't seem too much like the way we learned to do proofs in geometry, for example. An alternative is the construction of a logical argument which begins by assuming the hypotheses are all true and applies the basic rules of inferences from the table until the desired conclusion is shown to be true.

Here is an example of such a proof. Let's show that the argument displayed in figure 4.1 is valid.

$$\begin{array}{l} p \\ p \rightarrow q \\ s \vee r \\ \underline{r \rightarrow \neg q} \\ \therefore s \vee t \end{array}$$

Figure 4.1: A logical argument

Argument:	p	Proof:	(1) p	hypothesis
	$p \rightarrow q$		(2) $p \rightarrow q$	hypothesis
	$s \vee r$		(3) q	Modus Ponens (1) and (2)
	$\underline{r \rightarrow \neg q}$		(4) $r \rightarrow \neg q$	hypothesis
	$\therefore s \vee t$		(5) $q \rightarrow \neg r$	Logical equivalent of (4)
			(6) $\neg r$	Modus Ponens (3) and (5)
			(7) $s \vee r$	hypothesis
			(8) s	Disjunctive Syllogism (6) and (7)
			(9) $s \vee t$	Addition

Table 4.2 Proof of the validity of an argument

Each step in the argument will be justified in some way, either

- (1) as a hypothesis (and hence assumed to have truth value T), or
- (2) as a consequence of previous steps and some rule of inference from the table, or
- (3) as a statement logically equivalent to a previous statement in the proof.

Finally the last statement in the proof will be the desired conclusion. Of course, we could prove the argument valid by constructing a 32 row truth table instead! Well, actually we wouldn't need all 32 rows, but it would be pretty tedious in any case.

Such proofs can be viewed as games in which the hypotheses serve as the starting position in a game, the goal is to reach the conclusion as the final position in the game, and the rules of inference (and logical equivalences) specify the legal moves. Following this outline, we can be

sure every step in the proof is a true statement, and the desired conclusion is true, as we hoped to show.

One step more complicated than the last example are arguments that are presented in words rather than symbols. In such a case, it is necessary to first convert from a verbal argument to a symbolic argument, and then check the argument to see if it is valid. For example, consider the argument: *Tom is a cat. If Tom is a cat, then Tom likes fish. Either Tweety is a bird or Fido is a dog. If Fido is a dog, then Tom does not like fish. So, either Tweety is a bird or I'm a monkey's uncle.* Just reading this argument, it is difficult to decide if it is valid or not. It's just a little too confusing to process. But it is valid, and in fact it is the very same argument as given above. Let p be *Tom is a cat*, let q be *Tom likes fish*, let s be *Tweety is a bird*, let r be *Fido is a dog*, and let t be *I'm a monkey's uncle*. Expressing the statements in the argument in terms of p, q, r, s, t produces exactly the symbolic argument proved above.

Some logical arguments have a convincing ring to them but are nevertheless invalid. The classic example is an argument of the form *If it is snowing, then it is winter. It is winter. So it must be snowing.* A moment's thought is all that is needed to be convinced the conclusion does not follow from the two hypotheses. Indeed, there are many winter days when it does not snow. The error being made is called the **fallacy of affirming the conclusion**. In symbols, the argument is claiming that $[(p \rightarrow q) \wedge q] \rightarrow p$ is a tautology, but in fact, checking a truth table shows that it is not a tautology. Fallacies arise when statements that are not tautologies are treated as if they were tautologies.

Name	Instantiation Rules
Universal Instantiation	$\forall x P(x) \therefore P(c)$ if c is in the domain of x
Existential Instantiation	$\exists x P(x) \therefore P(c)$ for some c in the domain of x
Name	Generalization Rules
Universal Generalization	$P(c)$ for arbitrary c in the domain of $x \therefore \forall x P(x)$
Existential Generalization	$P(c)$ for some c in the domain of $x \therefore \exists x P(x)$

Table 4.3: Quantification Rules

Logical arguments involving propositions using quantifiers require a few more rules of inference. As before, these rules really amount to no more than a formal way to express common sense. For instance, if the proposition $\forall x P(x)$ is true, then certainly for every object c in the universe of discourse, $P(c)$ is true. After all, if the statement $P(x)$ is true for every possible choice of x , then, in particular, it is true when $x = c$. The other three rules of inference for quantified statements are just as obvious. All four quantification rules appear in table 4.3.

Example 4.2. *Let's analyze the following (fictitious, but obviously valid) argument to see how these rules of inference are used. All books written by Sartre are hard to understand. Sartre wrote a book about kites. So, there is a book about kites that is hard to understand. Let's use the following predicates to symbolize the argument:*

- 1) $S(x)$: x was written by Sartre.
- 2) $H(x)$: x is hard to understand.
- 3) $K(x)$: x is about kites.

The domain for x in each case is all books. In symbolic form the argument and a proof are

Argument: $\forall x (S(x) \rightarrow H(x))$

$$\underline{\exists x (S(x) \wedge K(x))}$$

$$\therefore \exists x (K(x) \wedge H(x))$$

<i>Proof:</i>	(1) $\exists x (S(x) \wedge K(x))$	Hypothesis
	(2) $S(c) \wedge K(c)$ for some c	Existential Instantiation (1)
	(3) $S(c)$	Simplification (2)
	(4) $K(c)$	Simplification (2)
	(5) $\forall x (S(x) \rightarrow H(x))$	Hypothesis
	(6) $S(c) \rightarrow H(c)$	Universal Instantiation (5)
	(7) $H(c)$	Modus Ponens (2) and (6)
	(8) $K(c) \wedge H(c)$	Conjunction (4) and (7)
	(9) $\exists x (K(x) \wedge H(x))$	Existential Generalization (8)

Exercises

Exercise 4.1. Show that $p \vee q$ and $\neg p \vee r, \therefore q \vee r$ is a valid rule of inference. It is called **Resolution**.

Exercise 4.2. Prove the following argument is valid. All Porsche owners are speeders. No owners of sedans buy premium fuel. Car owners that do not buy premium fuel never speed. So Porsche owners do not own sedans. Use all car owners as the domain of discourse.

Exercise 4.3. Prove the following symbolic argument is valid.

$$\begin{array}{l}
 \neg p \rightarrow (r \wedge \neg s) \\
 t \rightarrow s \\
 u \rightarrow \neg p \\
 \neg w \\
 \hline
 u \vee w \\
 \therefore \neg t \vee w
 \end{array}$$

Problems

Problem 4.1. Show that $p \rightarrow q$ and $\neg p, \therefore \neg q$ is not a valid rule of inference. It is called the *fallacy of denying the hypothesis*.

Problem 4.2. Prove that the following symbolic argument is valid.

$$\begin{array}{l} \neg p \wedge q \\ r \rightarrow p \\ \neg r \rightarrow s \\ \hline s \rightarrow t \\ \therefore t \end{array}$$

Problem 4.3. Prove that the following symbolic argument is valid.

$$\begin{array}{l} p \vee q \\ q \rightarrow r \\ (p \wedge s) \rightarrow t \\ \neg r \\ \hline \neg q \rightarrow (p \wedge s) \\ \therefore t \end{array}$$

Problem 4.4. Prove that the following symbolic argument is valid.

$$\begin{array}{l} (\neg p \vee q) \rightarrow r \\ s \vee \neg q \\ \neg t \\ p \rightarrow t \\ \hline (\neg p \wedge r) \rightarrow \neg s \\ \therefore \neg q \end{array}$$

Problem 4.5. Express the following argument in symbolic form and prove the argument is valid. If Ralph doesn't do his homework or he doesn't feel sick, then he will go to the party and he will stay up late. If he goes to the party, he will eat too much. He didn't eat too much. So Ralph did his homework.

Problem 4.6. In Problem 4.5, show that you can logically deduce that Ralph felt sick.

Problem 4.7. In Problem 4.5, can you logically deduce that Ralph stayed up late?

Problem 4.8. Show that the symbolic argument is valid.

$$\begin{array}{l} \exists x(A(x) \wedge \neg B(x)) \\ \hline \forall x(A(x) \rightarrow C(x)) \\ \therefore \exists x(C(x) \wedge \neg B(x)) \end{array}$$

Chapter 5: Sets: Basic Definitions

A **set** is a collection of objects. Often, but not always, sets are denoted by capital letters such as $A, B, \dots$ and the objects that make up a set, called its **elements**, are denoted by lowercase letters. Write $x \in A$ to mean that the object x is an element of A . If the object x is not an element of A , write $x \notin A$.

Two sets A and B are **equal**, written $A = B$ provided A and B comprise exactly the same elements. Another way to say the same thing: $A = B$ provided $\forall x (x \in A \Leftrightarrow x \in B)$.

There are a number of ways to specify a given set. We consider two of them.

One way to describe a set is to list its elements. This is called the **roster method**. Braces are used to signify when the list begins and where it ends, and commas are used to separate elements. For instance, $A = \{1, 2, 3, 4, 5\}$ is the set of positive whole numbers between 1 and 5 inclusive. It is important to note that the order in which elements are listed is immaterial. For example,

$\{1, 2\} = \{2, 1\}$ since $x \in \{1, 2\}$ and $x \in \{2, 1\}$ are both true for $x = 1$ and $x = 2$ and false for all other choices of x . Thus $x \in \{1, 2\}$ and $x \in \{2, 1\}$ always have the same truth value, and that means $\forall x (x \in \{1, 2\} \Leftrightarrow x \in \{2, 1\})$ is true. According to the definition of equality given above, it follows that $\{1, 2\} = \{2, 1\}$. The same sort of reasoning shows that repetitions in the list of elements of a set can be ignored. For example, $\{1, 2, 3, 2, 4, 1, 2, 3, 2\} = \{1, 2, 3, 4\}$. There is no point in listing an element of a set more than once.

The roster method has certain drawbacks. For example we probably don't want to list all of the elements in the set of positive integers between 1 and 99 inclusive. One option is to use an **ellipsis**. The idea is that we list elements until a pattern is established, and then replace the missing elements with $\dots$ (which is the ellipsis). So $\{1, 2, 3, 4, \dots, 99\}$ would describe our set.

The use of an ellipsis has one pitfall. It is **hoped** that whoever is reading the list will be able to guess the proper pattern and apply it to fill in the gap.

Another method to specify a set is via the use of **set-builder notation**. A set can be described in set-builder notation as $A = \{x | p(x)\}$. Here we read A is the set of all objects x for which the predicate $p(x)$ is true. So $\{1, 2, 3, 4, \dots, 99\}$ becomes $\{x | x \text{ is a whole number and } 1 \leq x \leq 99\}$.

Certain sets occur often enough that we have special notation for them.

$\mathbb{N} = \{x x \text{ is a non-negative whole number}\} = \{0, 1, 2, \dots\},$	the natural numbers.
$\mathbb{Z} = \{x x \text{ is a whole number}\} = \{\dots, -2, -1, 0, 1, 2, \dots\},$	the integers.
$\mathbb{Q} = \{x x = p/q, p, q \text{ integers and } q \neq 0\},$	the rational numbers.
$\mathbb{R} = \{x x \text{ is a real number}\},$	the real numbers.
$\mathbb{C} = \{x x = a + ib, a, b \in \mathbb{R}, i^2 = -1\}$	the complex numbers.

In addition to the above sets, there is a set with no elements, written as $\emptyset$ (also written using the roster style as $\{ \}$), and called the **empty set**. This set can be described using set builder style in many different ways. For example, $\{x \in \mathbb{R} | x^2 = -2\} = \emptyset$. In fact, if $P(x)$ is any predicate which is always false, then $\{x | P(x)\} = \emptyset$. There are two easy slips to make involving the empty set. First, don't write $\emptyset = 0$ (the idea being that both $\emptyset$ and 0 represent *nothing*). That is not correct since $\emptyset$ is a set, and 0 is a number, and it's not fair to compare two different types of objects. The other error is thinking $\emptyset = \{\emptyset\}$. This cannot be correct since the right-hand set has an element, but the left-hand set does not.

At the other extreme from the empty set is the **universal set**, denoted $\mathcal{U}$. The universal set consists of all objects under consideration in any particular discussion. For example, if the topic du jour is basic arithmetic then the universal set would be the set of all integers. Usually the universal set is left for the reader to guess. If the choice of the universal set is not an obvious one, it will be pointed out explicitly.

The set A is a **subset** of the set B , written as $A \subseteq B$, in case $\forall x(x \in A \rightarrow x \in B)$ is true. In plain English, $A \subseteq B$ if every element of A also is an element of B . So $\{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5\}$.

On the other hand $\{0, 1, 2, 3\} \not\subseteq \{1, 2, 3, 4, 5\}$ since 0 is an element of the left-hand set but not of the right-hand set. The meaning of $A \not\subseteq B$ can be expressed in symbols using De Morgan's law:

$$A \not\subseteq B \Leftrightarrow \neg(\forall x(x \in A \rightarrow x \in B)) \quad (5.1)$$

$$\equiv \exists x \neg(x \in A \rightarrow x \in B) \quad (5.2)$$

$$\equiv \exists x \neg(\neg(x \in A) \vee x \in B) \quad (5.3)$$

$$\equiv \exists x(x \in A \wedge x \notin B) \quad (5.4)$$

and the last line says $A \not\subseteq B$ if there is at least one element of A that is not an element of B .

The empty set is a subset of every set. To check that, suppose A is any set, and let's check to make sure $\forall x(x \in \emptyset \rightarrow x \in A)$ is true. But it is since for any x , the hypothesis of the implication $x \in \emptyset \rightarrow x \in A$ is F, and so the implication is T. So $\emptyset \subseteq A$. Another way to say the same thing is to notice that to claim $\emptyset \not\subseteq A$ is the same as claiming there is at least one element of $\emptyset$ that is not an element of A , but that is ridiculous, since $\emptyset$ has no elements at all.

To say that $A = B$ is the same as saying every element of A is also an element of B and every element of B is also an element of A . In other words, $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$, and this indicates the method by which the common task of showing two sets are equal is carried out: to show two sets are equal, show that each is a subset of the other.

If $A \subseteq B$, and $A \neq B$, A is a **proper subset** of B , denoted by $A \subset B$, or $A \subsetneq B$. In words, $A \subset B$ means every element of A is also an element of B and there is at least one element of B that is not an element of A . For example $\{1, 2\} \subset \{1, 2, 3, 4, 5\}$, and $\emptyset \subset \{1\}$.

A set is **finite** if the number of distinct elements in the set is a non-negative integer. In this case we call the number of distinct elements in the set its **cardinality** and denote this natural number

by $|A|$. For example, $|\{1, 3, 5\}| = 3$ and $|\emptyset| = 0$, $|\{\emptyset\}| = 1$, and $|\{\emptyset, \{a, b, c\}, \{X, Y\}\}| = 3$. A set, such as $\mathbb{Z}$, which is not finite, is **infinite**.

Given a set A the **power set of A** , denoted $\mathcal{P}(A)$, is the set of all subsets of A . For example, if $A = \{1, 2\}$, then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. It is not hard to see if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Exercises

Exercise 5.1. *List the members of the following sets.*

- a) $\{x \in \mathbb{Z} \mid 3 \leq x^3 < 100\}$
- b) $\{x \in \mathbb{R} \mid 2x^2 = 50\}$
- c) $\{x \in \mathbb{N} \mid 7 > x \geq 4\}$

Exercise 5.2. *Use set-builder notation to give a description of each set.*

- a) $\{-5, 0, 5, 10, 15\}$
- b) $\{0, 1, 2, 3, 4\}$
- c) *The interval of real numbers:* $[\pi, 4)$

Exercise 5.3. *Determine the cardinality of the sets in Exercises 5.1 and 5.2.*

Exercise 5.4. *Is the proposition Every element of the empty set has three toes true or false? Explain your answer.*

Exercise 5.5. *Determine the power set of $\{1, \{2\}\}$.*

Exercise 5.6. *True or false: $\{1, 2, 3, 4, 5\} = \{5, 2, 3, 1, 2, 1, 5, 4, 3, 2, 1\}$.*

Exercise 5.7. *True or false: The set of even integers is a subset of the set of integers that are multiples of four.*

Problems

Problem 5.1. *List the members of the following sets.*

- a) $\{x \in \mathbb{N} \mid 3 \leq x^2 < 100\}$
- b) $\{x \in \mathbb{Z} \mid 3 \leq x^2 < 100\}$
- c) $\{x \in \mathbb{R} \mid 0 < x \leq 5\}$
- d) $\{x \in \mathbb{N} \mid x^2 < 0\}$
- e) $\{1, \{1\}, \{1, 2\}\}$

Problem 5.2. *Determine the power set of $\{0, 1, 2\}$.*

Problem 5.3. *Determine the truth value of the following propositions:*

- a) *Every element of the empty set is positive.*
- b) *Some element of the empty set is positive.*
- c) $0 \in \emptyset$
- d) $0 = \emptyset$

Problem 5.4. *Determine the truth value of the following propositions:*

- a) *For any set A , $A \subseteq \mathcal{P}(A)$.*
- b) *For any set A , $A \in \mathcal{P}(A)$.*
- c) *For any finite set A , the cardinality of $\mathcal{P}(A)$ is greater than the cardinality of A .*

Problem 5.5. *Determine the cardinality of the following sets:*

- a) *The empty set.*
- b) *The power set of the empty set.*
- c) *The power set of the powerset of the empty set.*
- d) *The power set of $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.*
- e) $\{1, \{1\}, \{1, 2\}\}$.

Problem 5.6. *True or false:*

- a) *If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.*
- b) *If $n \in \mathbb{N}$, then $n - 1 \in \mathbb{N}$.*

Chapter 6: Set Operations

There are several ways of combining sets to produce new sets.

The **intersection** of A with B denoted $A \cap B$ is defined as $\{x | x \in A \wedge x \in B\}$. For example,

$$\{1, 2, 3, 4, 5\} \cap \{1, 3, 5, 7, 9\} = \{1, 3, 5\}.$$

So the intersection of two sets consists of the objects which are in both sets simultaneously. Two sets are **disjoint** if $A \cap B = \emptyset$.

Set operations can be visualized using **Venn diagrams**. A circle (or other closed curve) is drawn to represent a set. The points inside the circle are used to stand for the elements of the set. To represent the set operation of intersection, two such circles are drawn with an overlap to indicate the two sets may share some elements. In the Venn diagram, figure [6.1](#), the shaded area represents the intersection of A and B .

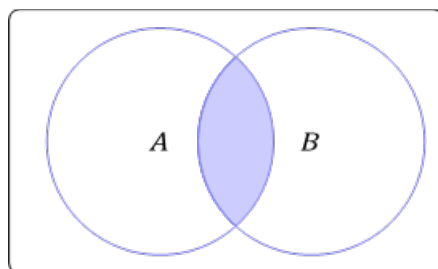


Figure 6.1: Venn diagram for $A \cap B$

The **union** of A with B denoted $A \cup B$ is $\{x | x \in A \vee x \in B\}$. In words, $A \cup B$ consists of those elements that appear in at least one of A and B . So

$$\{1, 2, 3, 4, 5\} \cup \{1, 3, 5, 7, 9\} = \{1, 2, 3, 4, 5, 7, 9\},$$

for example. The Venn Diagram [6.2](#) represents the union of A and B .

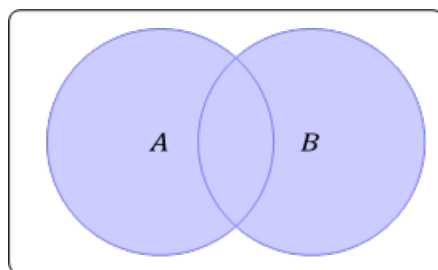


Figure 6.2 Venn diagram for $A \cup B$

The **symmetric difference** of A and B is defined to be $A \oplus B = \{x | x \in A \oplus x \in B\}$. So $A \oplus B$ consists of those elements which appear in exactly one of A and B . For example,

$$\{1, 2, 3, 4, 5\} \oplus \{1, 3, 5, 7, 9\} = \{2, 4, 7, 9\}.$$

The Venn diagram for the symmetric difference is figure 6.3.

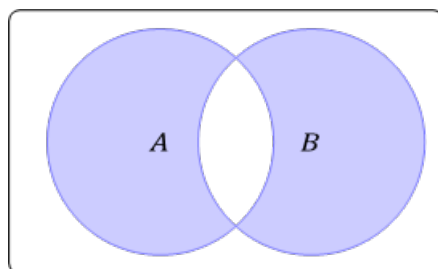


Figure 6.3: Venn diagram for $A \oplus B$

The **complement of B relative to A** , denoted $A - B$ is $\{x \mid x \in A \wedge x \notin B\}$. So

$$\{1, 2, 3, 4, 5\} - \{1, 3, 5, 7, 9\} = \{2, 4\}.$$

Figure 6.4 is the corresponding Venn diagram.

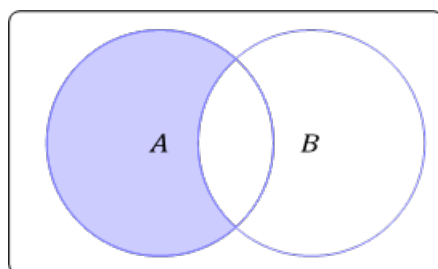


Figure 6.4: Venn diagram for $A - B$

When $\mathcal{U}$ is a universal set, we denote $\mathcal{U} - A$ by $\bar{A}$ and call it the **complement** of A . The Venn diagram for is in figure 6.5. If $\mathcal{U} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $\overline{\{0, 1, 2, 3, 4\}} = \{5, 6, 7, 8, 9\}$. The universal set matters here. If $\mathcal{U} = \{x \in \mathbb{N} \mid x \leq 100\}$, then $\overline{\{0, 1, 2, 3, 4\}} = \{5, 6, 7, \dots, 100\}$.

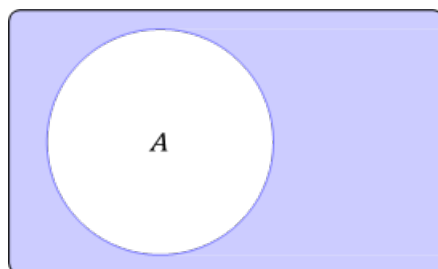


Figure 6.5: Venn diagram for $\bar{A} = \mathcal{U} - A$

There is a close connection between set operations and the logical connectives of Chapter 1. The intersection operation is related to conjunction, union is related to disjunction, and complementation is related to negation. It is not surprising then that the various laws of logic, such as the associative, commutative, and distributive laws carry over to analogous laws for the set operations. Table 6.1 exhibits some of these properties of these set operations.

These can be verified by using **membership tables** which are the analogs of truth tables used to verify the logical equivalence of propositions. For a set A either an element under consideration is in A or it is not. These binary possibilities are kept track of using 1 if $x \in A$ and 0 if $x \notin A$ and then performing related bit string operations.

Identity	Name
$\overline{(\bar{A})} = A$	Double Negation
$A \cap \mathcal{U} = A$ $A \cup \emptyset = A$	Identity Laws
$A \cap \emptyset = \emptyset$ $A \cup \mathcal{U} = \mathcal{U}$	Domination Laws
$A \cap A = A$ $A \cup A = A$	Idempotent Laws
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
$(A \cup B) \cup C = A \cup (B \cup C)$ $A \cap (B \cap C) = A \cap (B \cap C)$	Associative Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$	De Morgan's Laws
$A \cup \bar{A} = \mathcal{U}$	Law of Excluded Middle
$A \cap \bar{A} = \emptyset$	Law of Contradiction

Table 6.1: Laws of Set Theory

Example 6.1. Verify the De Morgan's law given by $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

The meaning of the first row of the table is that if $x \in A$ and $x \in B$, then $x \notin A \cap B$, as indicated by the 0 in the first row, fourth column, and also not in $A \cup B$ as indicated by the 0 in the first row, last column. Since the columns for $\overline{A \cap B}$ and $\bar{A} \cup \bar{B}$ are identical $\overline{A \cap B} = \bar{A} \cup \bar{B}$ follows.

A	B	$A \cap B$	$\overline{(A \cap B)}$	$\bar{A}$	$\bar{B}$	$\bar{A} \cup \bar{B}$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Table 6.2: Membership table for DeMorgan's law

Just as compound propositions can be analyzed using truth tables, more complicated combinations of sets can be handled using membership tables. For example, using a membership table, it is easy to verify that $\overline{A \cup (B \cap C)} = \bar{A} \cap (\bar{B} \cup \bar{C})$. But, just as with propositions, it is usually more enlightening to verify such equalities by applying the few basic laws of set theory listed above.

Example 6.2. *Let's prove $\overline{A \cup (B \cap C)} = \bar{A} \cap (\bar{B} \cup \bar{C})$*

Proof. The proof is just two applications of De Morgan's laws:

$$\overline{A \cup (B \cap C)} = \bar{A} \cap \overline{(B \cap C)} = \bar{A} \cap (\bar{B} \cup \bar{C}). \blacksquare$$

There is a correspondence between set operations of finite sets and bit string operations. Let

$$\mathcal{U} = \{u_1, u_2, \dots, u_n\}$$

be a finite universal set with distinct elements listed in a specific order. Notice the universal set is **ordered**. We may write it as an n -tuple: $\mathcal{U} = (u_1, u_2, \dots, u_n)$. For a set A under consideration, we have $A \subseteq \mathcal{U}$. By the law of excluded middle, for each $u_j \in \mathcal{U}$, either $u_j \in A$ or $u_j \notin A$. We define a binary string of length n , called the **characteristic vector** of A , denoted $\chi(A)$, by setting the j th bit of $\chi(A)$ to be 1 if $u_j \in A$ and 0 if $u_j \notin A$. For example, if $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and $A = \{1, 3, 4, 5, 8\}$, then $\chi(A) = 101110010$.

An interesting side-effect is that $\chi(A \cap B) = \chi(A) \wedge \chi(B)$, $\chi(A \cup B) = \chi(A) \vee \chi(B)$ and $\chi(\bar{A}) = \neg \chi(A)$. As a function, we say that χ maps intersection to conjunction.

Since every proposition can be expressed using $\wedge$, $\vee$ and $\neg$, if we represent sets by their characteristic vectors, we can get a machine to perform set operations as logical operations on bit strings. This is the method programmers use to manipulate sets in computer memory.

The order in which elements of a set are listed does not matter. But there are times when order is important. For example, in a horse race, knowing the order in which the horses cross the finish line is more interesting than simply knowing which horses were in the race. There is a familiar way, introduced in algebra, of indicating order is important: ordered pairs. Ordered pairs of numbers are used to specify points in the Euclidean plane when graphing functions. For instance, when graphing $y = 2x + 1$, setting $x = 3$ gives $y = 7$, and so the ordered pair $(3, 7)$ will indicate one of the points on the graph.

In this course, ordered pairs of any sorts of objects, not just numbers, will be of interest. An **ordered pair** is a collection of two objects (which might both be the same) with one specified as first (the first coordinate) and the other as second (the second coordinate). The ordered pair with a specified as first and b as second is written (as usual) (a, b) . The most important feature of ordered pairs is that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. In words, two ordered pairs are equal provided they match in both coordinates. So $(1, 2) \neq (2, 1)$.

More generally, an **ordered n -tuple** $(a_1, a_2, \dots, a_n)$ is the ordered collection with a_1 as its first coordinate, a_2 as its second coordinate, and so on. Two ordered n -tuples are equal provided they match in every coordinate.

The last operation to be considered for combining sets is the **Cartesian product** of two sets A and B . It is defined by $A \times B = \{(a, b) | a \in A \wedge b \in B\}$. In other words, $A \times B$ comprises all ordered pairs that can be formed taking the first coordinate from A and the second coordinate

from B . So if $A = \{1, 2\}$, and $B = \{\alpha, \beta\}$, then $A \times B = \{(1, \alpha), (2, \alpha), (1, \beta), (2, \beta)\}$. Notice that in this case $A \times B \neq B \times A$ since, for example, $(1, \alpha) \in A \times B$, but $(1, \alpha) \notin B \times A$.

A special case occurs when $A = B$. In this case we denote the Cartesian product of A with itself by A^2 . The familiar example $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is called the Euclidean plane or the Cartesian plane.

More generally given sets $A_1, \dots, A_n$ the Cartesian product of these sets is written as

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) | a_i \in A_i, 1 \leq i \leq n\}.$$

Also A^n denotes the Cartesian product of A with itself n times.

To avoid the use of an ellipsis we also denote the Cartesian product of $A_1, \dots, A_n$ as

$$\prod_{k=1}^n A_k$$

The variable k is called the **index** of the product. Most often the index is a whole number. Unless we are told otherwise we start with $k = 1$ and increment k by 1 successively until we reach n . So if we are given A_1, A_2, A_3, A_4 and A_5 , then

$$\prod_{k=1}^5 A_k = A_1 \times A_2 \times A_3 \times A_4 \times A_5.$$

Exercises

Exercise 6.1. Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and $B = \{1, 2, 4, 6, 7, 8, 9\}$. Find

- a) $A \cap B$
- b) $A \cup B$
- c) $A - B$
- d) $B - A$

Exercise 6.2. Determine the sets A and B given that $A - B = \{1, 2, 7, 8\}$, $B - A = \{3, 4, 10\}$ and $A \cap B = \{5, 6, 9\}$.

Exercise 6.3. Use membership tables to show that $A \oplus B = (A \cup B) - (A \cap B)$.

Exercise 6.4. Verify $A \oplus B = (A \cup B) - (A \cap B)$ using Venn diagrams.

Exercise 6.5. Verify $A \cup (A \cap B) = A$ using the rules of set algebra.

Exercise 6.6. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{\alpha, \beta\}$, and $D = \{7, 8, 9\}$. Write out the following Cartesian products.

- a) $A \times B$
- b) $B \times A$
- c) $C \times B \times D$

Exercise 6.7. What can you conclude about A and B if $A \times B = B \times A$.

Exercise 6.8. If $\mathcal{U} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, determine $\chi(\{1, 2, 4, 8\})$.

Exercise 6.9. Let $A = \{1, 2, 3\} \times \{1, 2, 3, 4\}$. List the elements in the set

$$B = \{(s, t) \in A \mid s \geq t\}.$$

Problems

Problem 6.1. Let $A = \{1, 2, 3, 5, 6, 7, 9\}$ and $B = \{1, 3, 4, 6, 8, 9\}$. Find

- a) $A \cap B$
- b) $A \cup B$
- c) $A - B$
- d) $B - A$

Problem 6.2. Use the rules of set algebra to verify $A \oplus B = (A \cup B) - (A \cap B)$.

Problem 6.3. Let $A = \{1, 2, 3\} \times \{1, 2, 3, 4\}$. List the elements of the set

$$B = \{(s, t) \in A \mid s < t\}.$$

Problem 6.4. Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \times \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

- a) What is the cardinality of A ?
- b) What is the cardinality of $A \times A$?
- c) What is the cardinality of $B = \{s \mid (s, s^2) \in A\}$?

Problem 6.5. True or False:

- a) For all sets A, B, C , $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
- b) For all sets A, B, C , $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
- c) For all sets A, B, C, D , $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.
- d) For all sets A, B, C, D , $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$.

Problem 6.6. Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Find $\chi(\{1, 2, 3, 4\})$.

Chapter 7: Styles of Proof

Earlier, we practiced proving the validity of logical arguments, both with and without quantifiers. The technique introduced there is one of the main tools for constructing proofs in a more general setting. In this chapter, various common styles of proof in mathematics are described.

Recognizing these styles of proof will make both reading and constructing proofs a little less onerous. The example proofs in this chapter will use some familiar facts about integers, which we will prove in a later chapter.

As mentioned before, the typical form of the statement of a theorem is: *if a and b and c and $\dots$, then d* . The propositions $a, b, c, \dots$ are called the hypotheses, and the proposition d is called the conclusion. The goal of the proof is to show that $(a \wedge b \wedge c \wedge \dots) \rightarrow d$ is a true proposition. In the case of propositional logic, the only thing that matters is the *form* of a logical argument, not the particular propositions that are involved. That means the proof can always be given in the form of a truth table. In areas outside of propositional logic that is no longer possible. Now the content of the propositions must be considered. In other words, what the words mean, and not merely how they are strung together, becomes important.

Suppose we want to prove an implication **Theorem:** *If p , then q* . In other words, we want to show $p \rightarrow q$ is true. There are two possibilities: Either p is false, in which case $p \rightarrow q$ is automatically true, or p is true. In this second case, we need to show that q is true as well to conclude $p \rightarrow q$ is true. In other words, to show $p \rightarrow q$ is true, we can begin by assuming p is true, and then give an *argument* that q must be true as well. The outline of such a proof will look like:

Proof.	Step 1	Reason 1
	Step 2	Reason 2
	$\vdots$	$\vdots$
	Step m	Reason m ■

The symbol ■ in the last line informs the reader that the proof is finished. Every step in the proof must be a true proposition, and since the goal is to conclude q is true, the proposition q will be the last step in the proof. **There are only four acceptable reasons** that can be invoked to justify a step in a proof. Each step can be: (1) a *hypothesis* (and so assumed to be true), (2) an application of a *definition*, (3) a *known fact* proved previously, and so known to be true, or (4) a consequence of applying a *rule of inference* or a *logical equivalence* to earlier steps in the proof. The only difference between these sorts of formal proofs and the proofs of logical arguments we practiced earlier is the inclusion of definitions as a justification of a step.

Before giving a few examples, there is one more point to consider. Most theorems in mathematics involve variables in some way, along with either universal or existential quantifiers. But, in the case of universal quantifiers, tradition dictates that the mention of the quantifier is

often suppressed, and left for the reader to fill in. For example consider: **Theorem:** *If n is an even integer, then n^2 is an even integer.* The statement is really shorthand for **Theorem:** *For every $n \in \mathbb{Z}$, if n is even, then n^2 is even.* If we let $E(n)$ be the predicate n is even with universe of discourse $\mathbb{Z}$, the theorem becomes **Theorem:** $\forall n(E(n) \rightarrow E(n^2))$. The truth of such a universally quantified statement can be accomplished with an application of the rule of universal generalization. In other words, we prove that for an arbitrary $n \in \mathbb{Z}$, the proposition $E(n) \rightarrow E(n^2)$ is true.

Theorem 7.1. *If n is an even integer, then n^2 is an even integer.*

Proof.

1) n is an even integer	hypothesis
2) $n = 2k$ for an integer k	definition of even
3) $n^2 = 4k^2$	algebra fact
4) $n^2 = 2(2k^2)$	algebra fact
5) n^2 is even	definition of even ■

Usually proofs are not presented in the dry step-wise style of the last example. Instead, a more narrative style is used. So the above proof could go as follows:

Theorem 7.2. *If n is an even integer, then n^2 is an even integer.*

Proof. Suppose n is an even integer. That means $n = 2k$ for some integer k . Squaring both sides gives $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which shows n^2 is even. ■

All the ingredients of the step-wise proof are present in the narrative form, but this second form is a little more reader friendly. For example, we can include a few comments, such as *squaring both sides* gives to help the reader figure out what is happening.

The method of proof given above is called **direct proof**. The characteristic feature of a direct proof is that in the course of the proof, the hypotheses appear as steps, and the last step in the proof is the conclusion of the theorem.

Here is one more example of a direct proof.

Theorem 7.3. *If n and m are odd integers, then $n + m$ is even.*

Proof. Suppose m and n are odd integers. That means $m = 2j + 1$ and $n = 2k + 1$ for some integers j and k . Adding gives

$$m + n = (2j + 1) + (2k + 1) = 2j + 2k + 2 = 2(j + k + 1),$$

and so $m + n$ is even since $j + k + 1$ is an integer. ■

There are situations where a direct proof is not very convenient for one reason or another. There are several other styles of proof, each based on some logical equivalence.

For example, since $p \rightarrow q \equiv \neg q \rightarrow \neg p$, we can prove the

Theorem 7.4. $p \rightarrow q$

by instead giving a proof of

Theorem 7.5. $\neg q \rightarrow \neg p$.

In other words, we replace the requested implication with its contrapositive and prove that instead. This method of proof is called **indirect proof**. Here's an example. **Theorem 7.6.** *If m^2 is an even integer, then m is an even integer.*

Proof. Suppose m is not even. Then m is odd. So $m = 2k + 1$ for some integer k . Squaring both sides of that equation gives $m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which shows that m^2 is not an even integer. ■

Notice that we gave a *direct proof* of the equivalent theorem: *If m is not an even integer, then m^2 is not an even integer.*

Another alternative to a direct proof is **proof by contradiction**. In this method the plan is to replace the requested **Theorem:** r (where r can be any simple or compound proposition) with **Theorem:** $\neg r \rightarrow \mathbb{F}$, where $\mathbb{F}$ is any proposition known to be false. The reason proof by contradiction is a valid form of proof is that $\neg r \rightarrow \mathbb{F} \equiv r$, so that showing $\neg r \rightarrow \mathbb{F}$ is true is identical to showing r is true. Proofs by contradiction can be a bit more difficult to discover than direct or indirect proofs. The reason is that in those two types of proof, we know exactly what the last line of our proof will be. We know where we want to get to. But in a proof by contradiction, we only know that we want to end up with some (any) proposition known to be false. Typically, when writing a proof by contradiction, we experiment, trying various logical arguments, hoping to stumble across some false proposition, and so conclude the proof. For example, consider the following.

Theorem 7.7. $\sqrt{2}$ is irrational.

The plan is to replace the requested theorem with

Theorem 7.8. *If $\sqrt{2}$ is rational, then $\mathbb{F}$ (some fact known to be false).*

And now, we may give a direct proof of this replacement theorem:

Proof. Suppose that $\sqrt{2}$ is rational. Then there exist integers m and n with $n \neq 0$ so that $\sqrt{2} = m/n$, with m/n in lowest terms. Squaring both sides gives $2 = m^2/n^2$. Thus $m^2 = 2n^2$ and so m^2 is even. Therefore m is even. So $m = 2k$. Substituting $2k$ for m in $m^2 = 2n^2$ shows $(2k)^2 = 4k^2 = 2n^2$. Which means that $n^2 = 2k^2$. Therefore n^2 is even, which means that n is even. Now since both m and n are even, they have 2 as a common factor. Therefore m/n is in lowest terms and it is not in lowest terms. $\rightarrow \leftarrow$ ■

The symbol $\rightarrow\leftarrow$ (two arrows crashing into each other head on) denotes that we have reached a *fallacy* (F), a statement known to be false. It usually marks the end of a proof by contradiction.

In the next example, we will prove a proposition of the form $p \rightarrow q$ by contradiction. The theorem is about real numbers x and y .

Theorem 7.9. *If $0 < x < y$, then $\sqrt{x} < \sqrt{y}$.*

Think of the statement of the theorem in the form $p \rightarrow q$. The plan is to replace the requested theorem with

Theorem 7.10. $\neg(p \rightarrow q) \rightarrow \text{F}$.

But $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$. So we will actually prove $(p \wedge \neg q) \rightarrow \text{F}$. In other words, we will prove (directly)

Theorem 7.11. *If $0 < x < y$ and $\sqrt{x} \geq \sqrt{y}$, then F (some fallacy).*

Proof. Suppose $0 < x < y$ and $\sqrt{x} \geq \sqrt{y}$. Since $\sqrt{x} > 0$, $\sqrt{x}\sqrt{x} \geq \sqrt{x}\sqrt{y}$, which is the same as $x \geq \sqrt{xy}$. Also since $\sqrt{y} > 0$, $\sqrt{y}\sqrt{x} \geq \sqrt{y}\sqrt{y}$, which is the same as $\sqrt{xy} \geq y$. Putting $x \geq \sqrt{xy}$ and $\sqrt{xy} \geq y$ together, we conclude that $x \geq y$. Thus $x < y$ and $x \geq y$. $\rightarrow\leftarrow$ ■

The only other common style of proof is **proof by cases**. Let's first look at the justification for this proof technique. Suppose we are asked to prove

Theorem 7.12 (Theorem X). $p \rightarrow q$.

We *dream up* some propositions, r and s , and replace the requested theorem with three theorems:

Theorem 7.13 (Theorem XS).

- 1) $p \rightarrow (r \vee s)$,
- 2) $r \rightarrow q$, and
- 3) $s \rightarrow q$.

The propositions r, s we dream up are called the *cases*. There can be any number of cases. If we dream up three cases, then we would have four theorems to prove, and so on. The hope is that the proofs of these replacement theorems will be much easier than a proof of the original theorem. This is the *divide and conquer* approach to a proof.

The reason proof by cases is a valid proof technique is that

$$[(p \rightarrow (r \vee s)) \wedge (r \rightarrow q) \wedge (s \rightarrow q)] \rightarrow (p \rightarrow q)$$

is a tautology - which you should be able to verify. Proof by cases, as with proof by contradiction, is generally a little trickier than direct and indirect proofs. In a proof by contradiction, we are not sure exactly what we are shooting for. We just hope some contradiction

will pop up. For a proof by cases, we have to dream up the cases to use, and it can be difficult at times to dream up good cases.

Theorem 7.14. *For any integer n , $|n| \geq n$.*

Proof. Suppose n is an integer. There are two cases: Either (1): $n > 0$, or (2): $n \leq 0$. (This has the form $p \rightarrow (r \vee s)$ of (1) in Theorem 7.)

Case 1: We need to show *If $n > 0$, then $|n| \geq n$.* (We will do this with a direct proof.)

Suppose $n > 0$. Then $|n| = n$. Thus $|n| \geq n$ is true.

Case 2: We need to show *If $n \leq 0$, then $|n| \geq n$.* (We will again use a direct proof.)

Suppose $n \leq 0$. Now $0 \leq |n|$. Thus, $n \leq |n|$.

So in any case $n \leq |n|$ is true and that proves the theorem. ■

A proof of a statement of the form $\exists x P(x)$ is called an **existence proof**. The proof may be **constructive**, meaning that the proof provides a specific example of, or at least an explicit recipe for finding, an x so that $P(x)$ is true; or the proof may be **non-constructive**, meaning that it establishes the existence of x without giving a method of actually producing an example of an x for which $P(x)$ is true.

To give examples of each type of existence proof, let's use a familiar fact (which will be proved a little later in the course): There are infinitely many primes. Recall that a prime is an integer greater than 1 whose only positive divisors are 1 and itself. The next two theorems are contrived, but they demonstrate the ideas of constructive and nonconstructive proofs.

Theorem 7.15. *There is a prime with more than two digits.*

Proof. Checking shows that 101 has no positive divisors besides 1 and itself. Also, 101 has more than two digits. So we have produced an example of a prime with more than two digits. ■

Theorem 7.16. *There is a prime with more than one billion digits.*

Proof. Since there are infinitely many primes, they cannot all have one billion or fewer digits. So there must be some primes with more than one billion digits. ■

Finally, suppose we are asked to prove a theorem of the form $\forall x P(x)$, and for one reason or another we come to believe the proposition is not true. The proposition can be shown to be false by exhibiting a specific element from the domain of x for which $P(x)$ is false. Such an example is called a **counterexample** to the theorem. Let's look at a specific instance of the counterexample technique.

Theorem 7.17 (not really!). *For all positive integers n , $n^2 - n + 41$ is prime*

Counterexample 7.18. *To disprove the theorem, we explicitly specify a positive integer n such that $n^2 - n + 41$ is not prime. In fact, when $n = 41$, the expression is not a prime since clearly $41^2 - 41 + 41 = 41^2$ is divisible by 41. So, $n = 41$ is a counterexample to the proposition. ■*

An interesting fact about this example is that $n = 41$ is the smallest counterexample. For $n = 1, 2, \dots, 40$, it turns out that $n^2 - n + 41$ is a prime! This example shows the danger of checking a theorem of the form $\forall x P(x)$ for a few (or a few billion!) values of x , finding $P(x)$ true for those cases, and concluding it is true for every possible value of x .

Exercises

Exercise 7.1. Give a direct proof that the sum of two even integers is even.

Exercise 7.2. Give an indirect proof that if the square of the integer n is odd, then n is odd.

Exercise 7.3. Give a proof by contradiction that the sum of a rational number and an irrational number is irrational.

Exercise 7.4. Give a proof by contradiction that if $5n - 1$ is odd, then n is even.

Exercise 7.5. Give a counterexample to the proposition Every positive integer that ends with a 7 is a prime.

Problems

Problem 7.1. Give a direct proof that the sum of an even integer and an odd integer is odd. Hint: Start by letting m be an even integer and letting n be an odd integer. That means $m = 2k$ for some integer k and $n = 2j + 1$ for some integer j . You are interested in $m + n$, so add them up and see what you get. Why is the thing you get an odd integer (think about the definition of odd)?

Problem 7.2. Give a direct proof that the sum of two odd integers is even.

Problem 7.3. Give an indirect proof that if n^3 is even, then n is even. Hint: Study the solution of a similar statement in the sample exercises for this lesson.

Problem 7.4. Give a proof by contradiction that if $3n + 2$ is odd, then n is odd.

Hint: This is the problem in this set that gives the most grief. Study the section in the notes where the mechanics of proving a statement of the form If P , then Q by contradiction is discussed. Be sure you understand why the first line of the proof should be something like Suppose $3n + 2$ is odd and n is even.

Problem 7.5. Give an example of a predicate $P(n)$ about positive integers n , such that $P(n)$ is true for every positive integer from 1 to one billion, but which is never-the-less not true for all positive integers. (Hint: there is a really simple choice possible for the predicate $P(n)$.)

Problem 7.6. The **maximum** of two numbers, a and b is a provided $a \geq b$. Notation: $\max(a, b) = a$. The **minimum** of a and b is a provided $a \leq b$. Notation: $\min(a, b) = a$. Examples: $\max(2, 3) = 3$, $\max(5, 0) = 5$, $\min(2, 3) = 2$, $\min(5, 0) = 0$,

$\max(4, 4) = \min(4, 4) = 4$.

Give a proof by cases that for any numbers s, t , $\min(s, t) + \max(s, t) = s + t$.

Problem 7.7. Give a proof by cases that for integers m, n , we have $|mn| = |m||n|$.

Hint: Consider four cases: (1) $m \geq 0$ and $n \geq 0$, (2) $m \geq 0$ and $n < 0$, (3) $m < 0$ and $n \geq 0$, and (4) $m < 0$ and $n < 0$.

PART II: Relations and Functions

Chapter 8: Relations

Two-place predicates, such as $B(x, y)$: x is the brother of y , play a central role in mathematics. Such predicates can be used to describe many basic concepts. As examples, consider the predicates given verbally:

- (1) $G(x, y)$: x is greater than or equal to y which compares the magnitudes of two values.
- (2) $P(x, y)$: x has the same parity as y which compares the parity of two integers.
- (3) $S(x, y)$: x has square equal to y which relates a value to its square.

Two-place predicates are called **relations**, probably because of examples such as the *brother of* given above. To be a little more complete about it, if $P(x, y)$ is a two-place predicate, and the domain of discourse for x is the set A , and the domain of discourse for y is the set B , then P is called a **relation from A to B** . When working with relations, some new vocabulary is used. The set A (the domain of discourse for the first variable) is called the **domain** of the relation, and the set B (the domain of discourse for the second variable) is called the **codomain** of the relation.

There are several different ways to specify a relation. One way is to give a verbal description as in the examples above. As one more example of a verbal description of a relation, consider $E(x, y)$: *The word x ends with the letter y* . Here the domain will be words in English, and the codomain will be the twenty-six letters of the alphabet. We say the ordered pair (cat, t) **satisfies** the relation E , but that (dog, w) does not.

When dealing with abstract relations, a verbal description is not always convenient. An alternate method is to tell what the domain and codomain are to be, and then simply list the ordered pairs which will satisfy the relation. For example, if $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, then one of many possible relations from A to B would be $\{(1, b), (2, c), (4, c)\}$. If we name this relation R , we will write $R = \{(1, b), (2, c), (4, c)\}$. It would be tough to think of a natural verbal description of R .

When thinking of a relation, R , as a set of ordered pairs, it is common to write aRb in place of $(a, b) \in R$. For example, using the relation G defined above, we can convey the fact that the pair $(3, 2)$ satisfies the relation by writing any one of the following: (1) $G(3, 2)$ is true, (2) $(3, 2) \in G$, or (3) $3G2$. The third choice is the preferred one when discussing relations abstractly.

Sometimes the ordered pair representation of a relation can be a bit cumbersome compared to the verbal description. Think about the ordered pair form of the relation E given above:

$$E = \{(cat, t), (dog, g), (antidisestablishmentarianism, m), \dots\}.$$

Another way represent a relation is with a **graph**. Here, a graph is a diagram made up of dots, called **vertices**, some of which are joined by lines or curves, called **edges**. To draw a graph of a relation R from A to B , make a column of dots, one for each element of A , and label the dots with the names of those elements. Then, to the right of A 's column make a column of dots for the elements of B . Then connect the vertex labelled $a \in A$ to a vertex $b \in B$ with an edge provided $(a, b) \in R$. The diagram is called the **bipartite graph representation** of R .

Example 8.1. For the relation $R = \{(1, a), (2, b), (3, c), (3, d), (4, d)\}$ from $A = \{1, 2, 3, 4\}$ to $B = \{a, b, c, d\}$ a bipartite graph which represents R is given in figure [8.1](#).

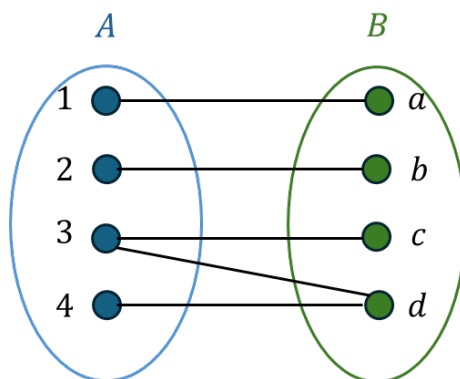


Figure 8.1: Bipartite graph representation of R

The choices made about the ordering and the placement of the vertices for the elements of A and B may make a difference in the appearance of the graph, but all such graphs are considered equivalent. Also, edges can be curved lines. All that matters is that such diagrams convey graphically the same information as R given as a set of ordered pairs.

It is common to have the domain and the codomain of a relation be the same set. If R is a relation from A to A , then we will say R is a **relation on A** . In this case there is a shorthand way of representing the relation by using a **digraph**. The word digraph is shorthand for *directed graph* meaning the edges have a direction indicated by an arrowhead. Each element of A is used to label a single point. An arrow connects the vertex labelled s to the one labelled t provided $(s, t) \in R$. An edge of the form (s, s) is called a **loop**.

Example 8.2. A digraph for the relation $R = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3), (3, 4), (4, 4)\}$ on the set $A = \{1, 2, 3, 4, 5\}$ is shown in figure [8.2](#).

Again it is true that a different placement of the vertices may yield a different-looking, but equivalent, digraph.

The last method for representing a relation is by using a $0 - 1$ matrix. This method is particularly handy for encoding a relation in computer memory. An $m \times n$ **matrix** is a rectangular array with m rows and n columns. Matrices are usually denoted by capital English letters. The entries of a matrix, usually denoted by lowercase English letters, are indexed by row and column. Either a_{ij} or $a_{i,j}$ stands for the entry in a matrix in the i th row and j th column. A $0 - 1$ **matrix** is one all of whose entries are 0 or 1. Given two finite sets A and B with m and n

elements respectively, we may use the elements of A (in some fixed order) to index the rows of an $m \times n, 0 - 1$ matrix, and use the elements of B to index the columns. So for a relation R from A to B , there is a matrix of R , M_R with respect to the orderings of A and B which represents R . The entry of M_R in the row labelled by a and column labelled by b is 1 if aRb and 0 otherwise. This is exactly like using characteristic vectors to represent subsets of $A \times B$, except that the vectors are cut into n chunks of size m .

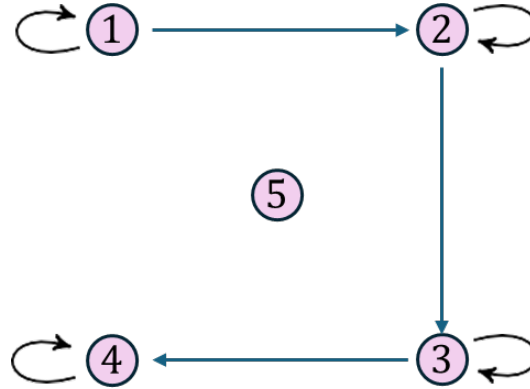


Figure 8.2: A digraph for the relation R

Example 8.3. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ and $R = \{(1, a), (1, b), (2, c), (4, c), (4, a)\}$. Then a 0–1 matrix which represents R using the natural orderings of A and B is given below. Note: This matrix may change appearance if A or B is listed in a different order.

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Since relations can be thought of as sets of ordered pairs, it makes sense to ask if one relation is a subset of another. Also, set operations such as union and intersection can be carried out with relations.

These notions can be expressed in terms of the matrices that represent the relations. Bit-wise operations on 0 – 1 matrices are defined in the obvious way. Then $M_{R \cup S} = M_R \vee M_S$, and $M_{R \cap S} = M_R \wedge M_S$. Also, for two 0 – 1 matrices of the same size $M \leq N$ means that wherever N has a 0 entry, the corresponding entry in M is also 0. Then $R \subseteq S$ means the same as $M_R \leq M_S$.

There are two new operations possible with relations.

First, if R is a relation from A to B , then by reversing all the ordered pairs in R , we get a new relation, denoted R^{-1} , called the **inverse** of R . In other words, R^{-1} is the relation from B to A given by $R^{-1} = \{(b, a) | (a, b) \in R\}$. A bipartite graph for R^{-1} can be obtained from a bipartite graph for R simply by interchanging the two columns of vertices with their attached edges (or, by rotating the diagram 180°).

If the matrix for R is M_R , then the matrix for R^{-1} is produced by taking the columns of $M_{R^{-1}}$ to be the rows of M_R . A matrix obtained by changing the rows of M into columns is called the **transpose** of M , and written as M^T . So, in symbols, if M is a matrix for R , then $M^T = M_{R^{-1}}$.

The second operation with relations concerns the situation when S is a relation from A to B and R is a relation from B to C . In such a case, we can form the **composition of S by R** which is denoted $R \circ S$. The composition is defined as

$$R \circ S = \{(a, c) | a \in A, c \in C \text{ and } \exists b \in B, \text{ such that } (a, b) \in S \text{ and } (b, c) \in R\}.$$

Example 8.4. Let $A = \{1, 2, 3, 4\}$, $B = \{\alpha, \beta\}$, $C = \{a, b, c\}$. $R = \{(\alpha, a), (\alpha, c), (\beta, b)\}$ and let $S = \{(1, \alpha), (1, \beta), (2, \alpha), (3, \beta), (4, \alpha)\}$. Since $(1, \alpha) \in S$ and $(\alpha, a) \in R$, it follows that the ordered pair $(1, a) \in R \circ S$. Likewise, since $(2, \alpha) \in S$ and $(\alpha, c) \in R$, we have $(2, c) \in R \circ S$. Continuing in that fashion shows that

$$R \circ S = \{(1, a), (1, b), (1, c), (2, a), (2, c), (3, b), (4, a), (4, c)\}.$$

The composition can also be determined by using the bipartite graphs of the relations. Make a column of vertices for A labelled 1, 2, 3, 4, then to the right a column of points for B labelled α, β , then again to the right a column of points for C labelled a, b, c . Draw in the edges as usual for R and S . (See figure 8.3.) Then a pair (x, y) will be in $R \circ S$ provided there is a two edge path from x to y .

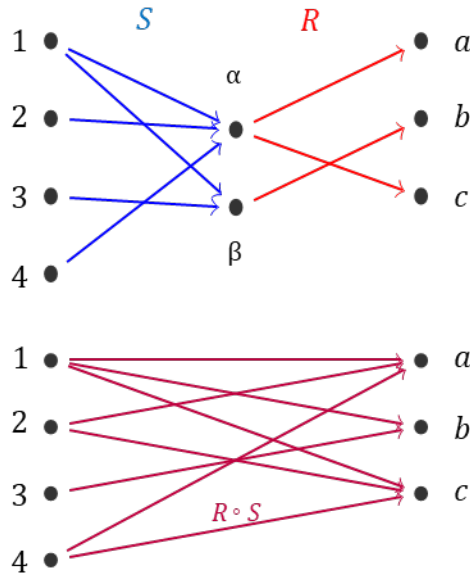


Figure 8.3: Graphical Presentation of $R \circ S$

From the picture it is instantly clear that, for example, $(1, c) \in R \circ S$.

In terms of 0–1 matrices if M_S is the $m \times k$ matrix of S with respect to the given orderings of A and B , and if M_R is the $k \times n$ matrix of R with respect to the given orderings of B and C , then whenever the i, l entry of S and l, j entry of R are both 1, then $(a_i, c_j) \in R \circ S$.

This example motivates the definition of the **Boolean product** of M_S and M_R as the corresponding matrix $M_{R \circ S}$ of the composition. More rigorously when M is an $m \times k$ 0–1 matrix and N is an $k \times n$ 0–1 matrix, $M \odot N$ is the $m \times n$ 0–1 matrix whose i, j entry is

$$(m_{i1} \wedge n_{1j}) \vee (m_{i2} \wedge n_{2j}) \vee \dots \vee m_{ik} \wedge n_{kj}.$$

This looks worse than it is. It achieves the desired result. The Boolean product is computed the same way as the ordinary matrix product where multiplication and addition have been replaced with $\wedge$ and $\vee$, respectively.

For the relations in the example above

$$M_{R \circ S} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = M_S \odot M_R$$

Exercises

Exercise 8.1. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (a, c), (b, b), (b, d), (c, a), (c, c), (d, b), (d, d)\}$ be a relation on A . Draw a digraph which represents R . Find the matrix which represents R **with respect to the ordering** (d, c, a, b) .

Exercise 8.2. The matrix of a relation S from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c, d\}$ with respect to the given orderings is displayed below. Represent S as a bipartite graph, and as a set of ordered pairs.

$$M_S = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Exercise 8.3. Find the composition $R \circ S$ (where R and S are defined in exercises [8.1](#) and [8.2](#)) as a set of ordered pairs. Use the Boolean product to find $M_{R \circ S}$ with respect to the natural orderings. N.B. The natural ordering for R is **not** the ordering used in exercise [8.1](#).

Exercise 8.4. Let $B = \{1, 2, 3, 4, 5, 6\}$ and let

$R_1 = \{(1, 2), (1, 3), (1, 5), (2, 1), (2, 2), (2, 4), (3, 3), (3, 4), (4, 1), (4, 5), (5, 5), (6, 6)\}$ and

$R_2 = \{(1, 2), (1, 6), (2, 1), (2, 2), (2, 3), (2, 5), (3, 1), (3, 3), (3, 6), (4, 2), (4, 3), (4, 4), (5, 1), (5, 5), (5, 6), (6, 2), (6, 3), (6, 6)\}.$

(a) Find $R_1 \cup R_2$, $R_1 \cap R_2$, and $R_1 \oplus R_2$.

(b) With respect to the given ordering of B find the matrix of each relation in part (a)

Problems

Problem 8.1. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (a, c), (b, d), (c, a), (c, c), (d, b)\}$ be a relation on A . Draw a digraph which represents R . Draw a bipartite graph which represents R .

Problem 8.2. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (a, c), (b, d), (c, a), (c, c), (d, b)\}$ be a relation on A . What is the inverse of R ?

Problem 8.3. Find the composition, $R \circ S$, where $S = \{(1, a), (4, a), (5, b), (2, c), (5, c), (3, d)\}$ and $R = \{(a, x), (a, y), (b, x), (c, z), (d, z)\}$, as a set of ordered pairs.

Problem 8.4. Find $R_1 \cup R_2$ and $R_1 \cap R_2$ where $R_1 = \{(1, 2), (1, 3), (1, 5), (2, 1), (6, 6)\}$ and $R_2 = \{(1, 2), (1, 6), (3, 6), (4, 2), (5, 6), (6, 2), (6, 3)\}$.

Problem 8.5. Let L be the relation less than on the set of integers. Examples $3L7$ and $-8L0$ are true, but $5L2$ and $6L6$ are false. How would describe the relation L^{-1} ?

Problem 8.6. True or False: For any relation R , $(R^{-1})^{-1} = R$. Explain your answer.

Problem 8.7. Are there relations R for which $R = R^{-1}$? If not, explain why it is not possible. If so, give an example of such a relation.

Problem 8.8. Let R be a relation on a set A and R^{-1} its inverse. Show that $(a, b) \in R \circ R^{-1}$ implies $(b, a) \in R \circ R^{-1}$.

Problem 8.9. Let A and B be two sets. Explain why the empty set, $\emptyset$, is a relation from A to B .

Problem 8.10. Let S be a relation from A to B , and let R be a relation from B to C . Prove that $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Chapter 9: Properties of Relations

There are several conditions that can be imposed on a relation R on a set A that make it useful. These requirements distinguish those relations which are interesting for some reason from the garden variety junk, which is, let's face it, what most relations are.

A relation R on A is **reflexive** provided $\forall a \in A, aRa$. In plain English, a relation is reflexive if every element of its domain is related to itself. The relation $B(x, y): x$ is the brother of y is not reflexive since no person is his own brother. On the other hand, the relation $S(m, n): m + n$ is even, is a reflexive relation on the set of integers since, for any integer $m, m + m = 2m$ is even.

In symbolic logic a relation R on a set A is reflexive means $(\forall a \in A)[aRa]$.

It is easy to spot a reflexive relation from its digraph: there is a loop at every vertex. Also, a reflexive relation can be spotted quickly from its matrix. First, let's agree that when the matrix of a relation on a set A is written down, the same ordering of the elements of A is used for both the row and column designators. For a reflexive relation, the entries on the **main diagonal** of its matrix will all be 1's. The main diagonal of a square matrix runs from the upper left corner to the lower right corner.

The flip side of the coin from reflexive is irreflexive. A relation R on A is **irreflexive** in case $(a, a) \notin R$ for all $a \in A$. In other words, no element of A is related to itself. The *brother of* relation is irreflexive. The digraph of an irreflexive relation contains no loops, and its matrix has all 0's on the main diagonal.

In symbols a relation R on a set A is irreflexive becomes

$$(\forall a \in A)[(a, a) \notin R] \equiv \neg(\exists a \in A)[aRa] \equiv \nexists a \in A, aRa.$$

Actually, that discussion was a little careless. To see why, consider the relation $S(x, y):$ **the square of** x is bigger than or equal to y .

Is this relation reflexive? The answer is: we can't tell. The answer depends on the domain of the relation, and we haven't been told what that is to be. For example, if the domain is the set $\mathbb{N}$ of natural numbers, then the relation is reflexive, since $n^2 \geq n$ for all $n \in \mathbb{N}$. However, if the domain is the set $\mathbb{R}$ of all real numbers, the relation is not reflexive. In fact, a counterexample to the claim that S is reflexive on $\mathbb{R}$ is the number $1/2$ since $(1/2)^2 = 1/4$ and $1/4 < 1/2$. The lesson to be learned from this example is that the question of whether a relation is reflexive cannot be answered until the domain has been specified. The same is true for the irreflexive condition and the other conditions defined below. Always be sure you know the domain before trying to determine which properties a relation satisfies.

A relation R on A is **symmetric** provided $(a, b) \in R \rightarrow (b, a) \in R$. Another way to say the same thing: R is symmetric provided $R = R^{-1}$. In words, R is symmetric provided that whenever a is related to b , then b is related to a . Any digraph representing a symmetric relation R will have a return edge for every non-loop. Think of this as saying the graph has no one-way streets. The matrix M of a symmetric relation satisfies $M = M^T$. In this case M is symmetric about its main

diagonal in the usual geometric sense of symmetry. The $B(x, y)$: x is the brother of y relation mentioned before is not symmetric if the domain is taken to be all people since, for example, $Donny B Marie$, but $(Marie, Donny) \notin B$. On the other hand, if we take the domain to be all (human) males, then B is symmetric.

In symbolic logic a relation R on a set A is symmetric means $(\forall a, b \in A)[aRb \rightarrow bRa]$.

A relation R on A is **antisymmetric** if whenever $(a, b) \in R$ and $(b, a) \in R$, then $a = b$. In other words, the only objects that are each related to the other are objects that are the same. For example, the usual $\leq$ relation for the integers is antisymmetric since if $m \leq n$ and $n \leq m$, then $n = m$. A digraph representing an antisymmetric relation will have all streets one-way except loops. If M is a matrix for R , then whenever $a_{i,j} = 1$ and $i \neq j, a_{j,i} = 0$.

In symbolic logic a relation R on A is antisymmetric means

$$(\forall a, b \in A)[(aRb) \wedge (bRa) \rightarrow (a = b)].$$

A relation R on A is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. This can also be expressed by saying $R \circ R \subseteq R$. In a digraph for a transitive relation whenever we have a directed path of length two from a to c through b , we must also have a direct link from a to c . This means that any digraph of a transitive relation has lots of triangles. This includes degenerate triangles where a, b and c are not distinct. A matrix M of a transitive relation satisfies the inequality $M \odot M \leq M$. The relation $\leq$ on $\mathbb{N}$ is transitive, since from $k \leq m$ and $m \leq n$, we can conclude $k \leq n$.

In symbolic logic a relation R on A is transitive means $(\forall a, b, c \in A)[(aRb) \wedge (bRc) \rightarrow (aRc)]$.

Example 9.1. Define a relation, N on the set of all living people by the rule $a N b$ if and only if a, b live within one mile of each other. This relation is reflexive since every person lives within a mile of himself. It is not irreflexive since I live within a mile of myself. It is symmetric since if a lives within a mile of b , then b lives within a mile of a . It is not antisymmetric since Mr. and Mrs. Smith live within a mile of each other, but they are not the same person. It is not transitive: to see why, think of the following situation (which surely exists somewhere in the world!): there is a straight road of length 1.5 miles. Say Al lives at one end of the road, Cal lives at the other end, and Sal lives halfway between Al and Cal. Then $Al N Sal$ and $Sal N Cal$, but not $Al N Cal$.

Example 9.2. Let $A = \mathbb{R}$ and define aRb iff $a \leq b$, then R is a reflexive, transitive, antisymmetric relation. Because of this example, any relation on a set that is reflexive, antisymmetric, and transitive is called an **ordering** relation. The subset relation on any collection of sets is another ordering relation.

Example 9.3. Let $A = \mathbb{R}$ and define aRb iff $a < b$. Then R is irreflexive, and transitive.

Example 9.4. If $A = \{1, 2, 3, 4, 5, 6\}$ then

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

is reflexive, symmetric, and transitive. In artificial examples such as this one, it can be a tedious chore checking that the relation is transitive.

Example 9.5. *If $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (1, 2), (2, 3), (1, 3), (3, 4), (2, 4), (4, 1)\}$ then R is not reflexive, not irreflexive, not symmetric, and not transitive but it is antisymmetric.*

Exercises

Exercise 9.1. Define a relation on $\{1, 2, 3\}$ which is both symmetric and antisymmetric.

Exercise 9.2. Define a relation on $\{1, 2, 3, 4\}$ by $R = \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4), (4, 3)\}$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show R satisfies the property or explain why it does not.

Exercise 9.3. Each matrix below specifies a relation R on $\{1, 2, 3, 4, 5, 6\}$ with respect to the given ordering 1, 2, 3, 4, 5, 6. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show R satisfies the property or explain why it does not.

$$\begin{array}{ll} \text{a) } \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} & \text{b) } \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \text{c) } \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} & \text{d) } \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Exercise 9.4. Define the relation $C(A, B): |A| \leq |B|$, where the domains for A and B are all subsets of $\mathbb{Z}$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show C satisfies the property or explain why it does not.

Exercise 9.5. Explain why $\emptyset$ is a relation on any set.

Exercise 9.6. Define the relation $M(A, B): |A \cap B| = 1$ (or, in plain English, A and B have exactly one element in common), where the domains for A and B are all subsets of $\mathbb{Z}$. A few examples:

- $\{5, 10\} M \{1, 2, 3, 4, 5, 6\}$ is true since the sets $\{5, 10\}$ and $\{1, 2, 3, 4, 5, 6\}$ have exactly one element in common (namely 5).
- It is true that $\{n | n \in \mathbb{Z} \text{ and } n \leq 0\} M \{n | n \in \mathbb{Z} \text{ and } n \geq 0\}$. Indeed, the unique common element of $\{n | n \in \mathbb{Z} \text{ and } n \leq 0\}$ and $\{n | n \in \mathbb{Z} \text{ and } n \geq 0\}$ is 0.
- $\{1, 2, 3\} M \{6, 7, 8, 9\}$ is false since $\{1, 2, 3\}$ and $\{6, 7, 8, 9\}$ have no common elements.

- $\{1, 2, 3, 4\} M \{2, 4, 6, 8\}$ is false since $\{1, 2, 3, 4\}$ and $\{2, 4, 6, 8\}$ have more than one element in common.

For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show M satisfies the property or explain why it does not.

Problems

Problem 9.1. Let R be the relation $\{(1, 1)\}$ on the set $A = \{1, 2\}$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show R satisfies the property or explain why it does not.

Problem 9.2. Let S be the relation $\{(1, 1), (1, 2), (1, 3), (2, 3)\}$ on the set $A = \{1, 2, 3\}$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show S satisfies the property or explain why it does not.

Problem 9.3. Let A be the relation on the set $\mathbb{Z}$ of all integers defined by sAt iff $|s| \leq |t|$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show A satisfies the property, or explain why it does not.

Problem 9.4. Let D be the relation on the natural numbers defined by the rule mDn if and only if m does not equal n . Examples: $5D7$ is true and $4D4$ is false. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show D satisfies the property or explain why it does not.

Problem 9.5. Let R be the relation $\{(1, 2), (2, 3), (3, 4)\}$ on the set $A = \{1, 2, 3\}$. The relation R is not transitive on A . What is the fewest number of ordered pairs that need to be added to R so it becomes a transitive relation on A ?

Problem 9.6. Give a counterexample to the claim that a relation R on a set A that is both symmetric and transitive must be reflexive. Hint: There is a very simple example!

Problem 9.7. Define the relation $M(A, B) : A \cap B = \emptyset$, where the domains for A and B are all subsets of $\mathbb{Z}$. For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show M satisfies the property or explain why it does not.

Problem 9.8.

- Let $A = \{1\}$, and consider the empty relation, $\emptyset$, on A . For each of the five properties of a relation defined in this chapter (reflexive, irreflexive, symmetric, antisymmetric, and transitive) either show $\emptyset$ satisfies the property or explain why it does not.
- Same question as (a), but now with $A = \emptyset$.

Chapter 10: Equivalence Relations

Relations capture the essence of many different mathematical concepts. In this chapter, we will show how to put the idea of *are the same kind* in terms of a special type of relation.

Before considering the formal concept of *same kind* let's look at a few simple examples.

Consider the question, posed about an ordinary deck of 52 cards: *How many different kinds of cards are there?* One possible answer is: *There are 52 kinds of cards*, since all the cards are different. But another possible answer in certain circumstances is: *There are four kinds of cards* (namely clubs, diamonds, hearts, and spades). Another possible answer is: *There are two kinds of cards, red and black*. Still another answer is: *There are 13 kinds of cards: aces, twos, threes, . . . , jacks, queens, and kings*. Another answer, for the purpose of many card games is: *There are ten kinds of cards, aces, twos, threes, up to nines, while tens, jacks, queens, and kings are all considered to be the same value (usually called 10)*. You can certainly think of many other ways to split the deck into a number of different kinds.

Whenever the idea of *same kind* is used, some properties of the objects being considered are deemed important and others are ignored. For instance, when we think of the the deck of cards made of the 13 different ranks, ace through king, we are agreeing the the suit of the card is irrelevant. So the jack of hearts and the jack of clubs are taken to be the same for what ever purposes we have in mind.

The mathematical term for *same kind* is **equivalent**. There are three basic properties always associated with the idea of equivalence.

- (1) *Reflexive*: Every object is equivalent to itself.
- (2) *Symmetric*: If object a is equivalent to object b , then b is also equivalent to a .
- (3) *Transitive*: If a is equivalent to b and b is equivalent to c , then a is equivalent to c .

To put the idea of equivalence in the context of a relation, suppose we have a set A of objects, and a rule for deciding when two objects in A are the same kind (equivalent) for some purpose. Then we can define a relation E on the set A by the rule that the pair (s, t) of elements of A is in the relation E if and only if s and t are the same kind. For example, consider again the deck of cards, with two cards considered to be the same if they have the same rank. Then a few pairs in the relation E would be (ace hearts, ace spades), (three diamonds, three clubs), (three clubs, three diamonds), (three diamonds, three diamonds), (king diamonds, king clubs), and so on.

Using the terminology of the previous chapter, this relation E , and in fact any relation that corresponds to notion of equivalence, will be reflexive, symmetric, and transitive. Thus, any reflexive, symmetric, transitive relation on a set A is called an **equivalence relation** on A .

Suppose E is an equivalence relation on a set A and that x is one particular element of A . The **equivalence class of x** is the set of all the things in A that are equivalent to x . The symbol used for the equivalence class of x is $[x]$, so the definition can be written in symbols as

$$[x] = \{y \in A \mid yEx\}.$$

For instance, think once more about the deck of cards with the equivalence relation *having the same rank*. The equivalence class of the two of spades would be the set $[2♠] = \{2♠, 2♦, 2♥, 2♣\}$. That would also be the equivalence class of the two of diamonds. On the other hand, if the equivalence relation we are using for the deck is *having the same suit*, then the equivalence class of the two of spades would be

$$[2♠] = \{A♠, 2♠, 3♠, 4♠, 5♠, 6♠, 7♠, 8♠, 9♠, 10♠, J♠, Q♠, K♠\}.$$

The most important fact about the collection of different equivalence classes for an equivalence relation on a set A is that they split the set A into separate pieces. In fancier words, they **partition** the set A . For example, the equivalence relation of having the same rank splits a deck of cards into 13 different equivalence classes. In a sense, when using this equivalence relation, there are only 13 different objects, four of each kind.

Here are a few more examples of equivalence relations.

Example 10.1. Define R on $\mathbb{N}$ by aRb if and only if $a = b$. In other words, equality is an equivalence relation. In fact, this example explains the choice of name for such relations.

Example 10.2. Let A be the set of logical propositions and define R on A by pRq iff $p \equiv q$.

Example 10.3. Let A be the set of people in the world and define R on A by aRb iff a and b are the same age in years.

Example 10.4. Let $A = \{1, 2, 3, 4, 5, 6\}$ and R be the relation on A with the matrix from exercise 3. part a) of chapter 9.

Example 10.5. Define P on $\mathbb{Z}$ by aPb if and only if a and b are both even, or both odd. We say a and b have the same parity.

For the equivalence relation *has the same rank* on a set of cards in a 52 card deck, there are 13 different equivalence classes. One of the classes contains all the aces, another contains all the 2's, and so on.

Example 10.6. For the equivalence relation from example [10.5](#), the equivalence class of 2 is the set of all even integers.

$$\begin{aligned} [2] &= \{n \mid 2Pn\} = \{n \mid 2 \text{ has the same parity as } n\} \\ &= \{n \mid n \text{ is even}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} \end{aligned}$$

In this example, there are two different equivalence classes, the one comprising all the even integers, and the other comprising all the odd integers. As far as parity is concerned, -1232215 and 171717 are the same.

Suppose E is an equivalence relation on A . The most important fact about equivalence classes is that every element of A belongs to exactly one equivalence class. Let's prove that.

Theorem 10.7. Let E be an equivalence relation on a set A , and let $a \in A$. Then there is exactly one equivalence class to which a belongs.

Proof. Let E be an equivalence relation on a set A , and suppose $a \in A$. Since E is reflexive, aEa , and so $a \in [a]$ is true. That proves that a is in at least one equivalence class. To complete the proof, we need to show that if $a \in [b]$ then $[b] = [a]$.

Now, stop and think: Here is what we know:

- (1) E is an equivalence relation on A ,
- (2) $a \in [b]$, and
- (3) the definition of equivalence class.

Using those three pieces of information, we need to show the two sets $[a]$ and $[b]$ are equal. Now, to show two sets are equal, we show they have the same elements. In other words, we want to prove

- (1) If $c \in [a]$, then $c \in [b]$, and
- (2) If $c \in [b]$, then $c \in [a]$.

Let's give a direct proof of (2).

Suppose $c \in [b]$. Then, according to the definition of $[b]$, $c E b$. The goal is to show $c \in [a]$. Now, we know $a \in [b]$, and that means $a E b$. Since E is symmetric and $a E b$, $b E a$ follows. Now we have $c E b$ and $b E a$. Since E is transitive, we can conclude $c E a$, and thus $c \in [a]$ as we hoped to show. That proves (2). ■

For homework, you will complete the proof of this theorem by doing part (1).

Definition 10.8. A **partition** of a set A is a collection of nonempty, pairwise disjoint subsets of A , so that A is the union of the subsets in the collection. For example $\{\{1, 2, 3\} \{4, 5, 6\}\}$ is a partition of $\{1, 2, 3, 4, 5, 6\}$. The subsets forming a partition are called the **parts of the partition**.

To express the meaning of theorem [10.7](#) above in different words: The different equivalence classes of an equivalence relation on a set partition the set into nonempty disjoint pieces. More briefly: the equivalence classes of E **partition** A .

The fact that an equivalence relation partitions the underlying set is reflected in the digraph of an equivalence relation. If we pick an equivalence class $[a]$ of an equivalence relation E on a finite set A and we pick $b \in [a]$, then $b E c$ for all $c \in [a]$. This is true since $a E b$ implies $b E a$ and if $a E c$, then transitivity fills in $b E c$. So, in any digraph for E every vertex of $[a]$ is connected to every other vertex in $[a]$ (including itself) by a directed edge. Also no vertex in $[a]$ is connected to any vertex in $A - [a]$. So the digraph of E consists of separate components, one for each distinct equivalence class, where each component contains every possible directed edge.

In terms of a matrix representation of an equivalence relation E on a finite set A of size n , let the distinct equivalence classes have size $k_1, k_2, \dots, k_r$, where $k_1 + \dots + k_r = n$. Next list the elements of A as $a_{11}, \dots, a_{k_1 1}, a_{12}, \dots, a_{k_2 2}, \dots, a_{1r}, \dots, a_{k_r r}$ where the i th equivalence class is $\{a_{1i}, \dots, a_{k_i i}\}$. Then the matrix for E with respect to this ordering is of the form

$$\begin{bmatrix} J_{k_1} & 0 & 0 & \dots & 0 \\ 0 & J_{k_2} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & J_{k_{r-1}} & 0 \\ 0 & \dots & 0 & 0 & J_{k_r} \end{bmatrix}$$

where J_{k_m} is the all 1's matrix of size $k_m \times k_m$. Conversely if the digraph of a relation can be drawn to take the above form, or if it has a matrix representation of the above form, then it is an equivalence relation and therefore reflexive, symmetric, and transitive.

Exercises

Exercise 10.1. Let $A = \{0, 1, 2\}$. Let $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Is R an equivalence relation on A ? If it is, what are the equivalence classes?

Exercise 10.2. Let $A = \{0, 1, 2, 3\}$. Let $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Is R an equivalence relation on A ? If it is, what are the equivalence classes?

Exercise 10.3. Let $A = \{0, 1, 2\}$. Let $R = \{(0, 0), (1, 1), (2, 2), (0, 1)\}$. Is R an equivalence relation on A ? If it is, what are the equivalence classes?

Exercise 10.4. Let $A = \{0, 1, 2\}$. Let $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0), (1, 2), (2, 1)\}$. Is R an equivalence relation on A ? If it is, what are the equivalence classes?

Exercise 10.5. True or False: The relation $R = \{(1, 1), (2, 2)\}$ on $A = \{1, 2\}$ is both symmetric and antisymmetric.

Exercise 10.6. The relation S is defined on the set $\mathbb{Z}$ of all integers by the rule $m S n$ if and only if $m^2 = n^2$. Is S an equivalence relation on $\mathbb{Z}$? If it is, what are the equivalence classes of S ?

Exercise 10.7. Let L be the collection of all straight lines in the plane. Four examples of elements in L : $x + y = 0, 2x - y = 5, x = 7, y = 0$. A relation C on L is defined by the rule $l_1 C l_2$ provided the lines l_1 and l_2 have at least one point in common. (The letter C should remind us of cross, and, loosely speaking, two lines are related if they cross each other. We will have to agree that a line crosses itself.) Is C an equivalence relation on L ? If it is, what are the equivalence classes of C ?

Exercise 10.8. Let R be a relation on a non-empty set A that is both symmetric, transitive. Also suppose that for each $a \in A$, aRb for at least one $b \in A$. Prove that R is reflexive, hence R is an equivalence relation.

Exercise 10.9. Let E be an equivalence relation on a set A , and let $a, b \in A$. Prove that either $[a] \cap [b] = \emptyset$ or else $[a] = [b]$.

Exercise 10.10. Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Form a partition of A using $\{1, 2, 4\}$, $\{3, 5, 7\}$, and $\{6, 8\}$. These are the equivalence classes for an equivalence relation E on A .

a) Draw a digraph for E .

b) Give a 0 – 1 matrix which represents E .

Exercise 10.11. Let $A = \{a, b, c, d, e, f, g, h\}$. Determine if each matrix represents an equivalence relation on A . If the matrix represents an equivalence relation find the equivalence classes. The natural ordering of the elements, a, b, c, d, e, f, g, h , is used to define the matrices.

$$(a) \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$(b) \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Exercise 10.12. Complete the proof of theorem [10.7](#) on page [61](#) by proving part (1).

Problems

Problem 10.1. Let A be the set of people alive on earth. For each relation defined below, determine if it is an equivalence relation on A . If it is, describe the equivalence classes. If it is not, determine which properties of an equivalence relation fail.

- a) $a H b$ if and only if a and b have the same height.
- b) $a G b$ if and only if a and b have a common grandparent.
- c) $a L b$ if and only if a and b have the same last name.
- d) $a N b$ if and only if a and b have a name (first name or last name) in common.
- e) $a W b$ if and only if a and b were born less than a day apart.

Problem 10.2. Let L be the collection of all straight lines in the plane. Four examples of elements in L : $x + y = 0$, $2x - y = 5$, $x = 7$, $y = 0$. A relation P on L is defined by the rule that $l_1 P l_2$ provided the lines l_1 and l_2 are parallel. Is P an equivalence relation on L ? If it is, what are the equivalence classes of P ?

Problem 10.3. Consider the relation $S(x, y)$: x is a sibling of y on the set A of people alive on earth. Is S reflexive? Is S symmetric? Is S transitive? (To be precise, siblings will mean two different people with the same two parents. Don't consider half-siblings for this problem.)

Problem 10.4. The relation $R = \{(a, a), (a, b)\}$ is not an equivalence relation on the set $A = \{a, b, c\}$. What is the fewest number of ordered pairs that need to be added to R so the result is an equivalence relation on A ?

Problem 10.5. Let A be the set of all ordered pairs of positive integers. Some members of A are $(3, 6)$, $(7, 7)$, $(11, 4)$, $(1, 2981)$. A relation R on A is defined by the rule $(a, b)R(c, d)$ if and only if $ad = bc$. For example $(3, 5)R(6, 10)$ is true since $(3)(10) = (5)(6)$.

- a) Explain why R is an equivalence relation on A .
- b) List four ordered pairs in the equivalence class of $(2, 3)$.

Problem 10.6. Let $A = \{1, 2, 3, 4, 5, 6\}$. Form a partition of A using $\{1, 2\}$, $\{3, 4, 5\}$, and $\{6\}$. These are the equivalence classes for an equivalence relation E on A . Draw the **digraph** of E .

Problem 10.7. Let $A = \{1, 2, 3\}$. The relation $E = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$ is an equivalence relation on A . The relation $F = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$ is also an equivalence relation on A . Compute the composition $F \circ E$. Is $F \circ E$ an equivalence relation on A ?

Chapter 11: Functions and Their Properties

In algebra, functions are thought of as formulas such as $f(x) = x^2$ where x is any real number. This formula gives a rule that describes how to determine one number if we are handed some number x . So, for example, if we are handed $x = 2$, the function f says that determines the value 4, and if we are handed 0, f says that determines 0. There is one condition that, by mutual agreement, such a function rule must obey to earn the title function: the rule must always determine *exactly one value* for each (reasonable) value it is handed. Of course, for the example above, $x = \text{blue}$ isn't a reasonable choice for x , so f doesn't determine a value associated with *blue*. The **domain** of this function is all real numbers.

Instead of thinking of a function as a formula, we could think of a function as any rule which determines exactly one value for every element of a set A . For example, suppose W is the set of all words in English, and consider the rule, I , which associates with each word, w , the first letter of w . Then $I(\text{cat}) = c$, $I(\text{dog}) = d$, $I(a) = a$, and so on. Notice that for each word w , I always determines exactly one value, so it meets the requirement of a function mentioned above. Notice that for the same set of all English words, the rule $T(w)$ is the third letter of the word w is not a function since, for example, $T(\text{be})$ has no value.

Here is the semi-formal definition of a function: A **function** from the set A to the set B is any rule which describes how to determine exactly one element of B for each element of A . The set A is called the **domain** of f , and the set B is called the **codomain** of f . The notation $f: A \rightarrow B$ means f is a function from A to B .

There are cases where it is not convenient to describe a function with words or formulas. In such cases, it is often possible to simply make a table listing the members of the domain along with the associated member of the codomain.

Example 11.1. Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{a, b, c, d, e\}$ and let $f: A \rightarrow B$ be specified by table [11.1](#).

x	$f(x)$
1	a
2	a
3	c
4	b
5	d
6	e

Table 11.1: A simple function

It is hard to imagine a verbal description that would act like f , but the table says it all. It is traditional to write such tables in a more compact form as

$$f = \{(1, a), (2, a), (3, c), (4, b), (5, d), (6, e)\}.$$

The last result in example [11.1](#) looks like a relation, and that leads to the modern definition of a function:

Definition 11.2. A function, f , with domain A and codomain B is a relation from A to B (hence $f \subseteq A \times B$) such that each element of A is the first coordinate of exactly one ordered pair in f .

That completes the evolution of the concept of function from formula, through rule, to a set of ordered pairs. With functions, by tradition we write $b = f(a)$ instead of $(a, b) \in f$.

In algebra and calculus, the functions of interest have a domain and a codomain consisting of sets of real numbers, $A, B \subseteq \mathbb{R}$. The *graph* of f is the set of ordered pairs in the Cartesian plane of the form $(x, f(x))$. Normally in this case, the output of the function f is determined by some formula. For example, $f(x) = x^2$.

We can spot a function in this case by the **vertical line test**. A relation from a subset A of $\mathbb{R}$ to another subset of $\mathbb{R}$ is a function if every vertical line of the form $x = a$, where $a \in A$ intersects the graph of f exactly once.

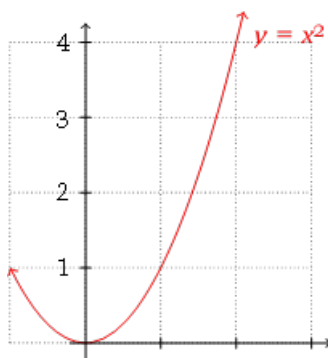


Figure 0-11.1: Graph of $y = x^2$

In discrete mathematics, most functions of interest have a domain and codomain some finite sets, or perhaps a domain or codomain consisting of integers. Such domains and codomains are said to be **discrete**.

When $f: A \rightarrow B$ is a function and both A and B are finite, then since f is a relation, we can represent f either as a 0 – 1 matrix or a bipartite graph. If M is a 0 – 1 matrix which represents a function, then since every element of A occurs as the first entry in exactly one ordered pair in f , it must be that every row of M has exactly one 1 in it. So it is easy to distinguish which relations are functions, and which are not from the matrix for the relation. This is the discrete analog of the vertical line test, (but notice that rows are horizontal).

Example 11.3. Again, let's consider the function defined, as in example [11.1](#), where f is from $A = \{1, 2, 3, 4, 5, 6\}$ to $B = \{a, b, c, d, e\}$ and given by the relation

$$f = \{(1, a), (2, a), (3, c), (4, b), (5, d), (6, e)\}.$$

If we take the given orderings of A and B , then the 0 – 1 matrix representing the function f appears in figure [11.2](#).

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 11.2: A function in 0 – 1 matrix form

Notice that in matrix form the number of 1's in a column coincides with the number of occurrences of the column label as output of the function. So, the sum of all entries in a given column equals the number of times the element labeling that column is an output of the function.

When a function from A to B is represented as a bipartite graph, every vertex of A is connected to exactly one element of B .

In the case of a function whose domain is a subset of $\mathbb{R}$, the number of times that the horizontal line $y = b$ intersects the graph of f , is the number of inputs from A for which the function value is b . Notice that these criteria are twisted again. In the finite case we are now considering vertical information, and in the other case we are considering horizontal information. In either case, these criteria will help us determine which of several special properties a function either has or lacks.

We say that a function $f: A \rightarrow B$ is **one-to-one** provided $f(s) = f(t)$ implies $s = t$. A more sophisticated word for one-to-one is **injective**. The definition can also be expressed in the contrapositive as: f is one-to-one provided $s \neq t$ implies $f(s) \neq f(t)$. But the definition is even easier to understand in words: a function is one-to-one provided different inputs always result in different outputs. For example, consider the function $f: \mathbb{R} \rightarrow \mathbb{R}$ given by the formula $f(x) = x^2$. This function is not one-to-one since both inputs 2 and -2 are associated with the same output: $f(2) = 2^2 = 4$ and $f(-2) = (-2)^2 = 4$.

Example 11.4. Proving a function is one-to-one can be a chore. Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = x^3 - 2$. Let's prove f is one-to-one.

Proof. Suppose $f(s) = f(t)$, then $s^3 - 2 = t^3 - 2$. Thus $s^3 = t^3$. So $s^3 - t^3 = 0$. Now $s^3 - t^3 = (s - t)(s^2 + st + t^2)$ implies $s - t = 0$ or $s^2 + st + t^2 = 0$. The first case leads to $s = t$. Using the quadratic formula, the second case leads to $s = -t + \frac{\sqrt{t^2 - 4t^2}}{2}$. Since s has to be a real number, the expression under the radical cannot be negative. The only other option is that it is zero, and that means $t = 0$. Of course, if $t = 0$ this leads to $s = 0 = t$. So, in any case, $s = t$. ■

The one-to-one property is very easy to spot from either the matrix or the bipartite graph of a function. When $f: A \rightarrow B$ is one-to-one, and $|A| = m$ and $|B| = n$ for some $m, n \in \mathbb{N} - \{0\}$, then when f is represented by a 0–1 matrix M , there can be no more than one 1 in any column.

So the column sums of any $0 - 1$ matrix representing a one-to-one function are all less than or equal to 1.

Since every row sum of M is 1 and there are m rows, we must have $m \leq n$. The bipartite graph of a one-to-one function can be recognized by the feature that no vertex of the codomain has more than one edge leading to it.

We say that a function $f: A \rightarrow B$ is **onto**, or **surjective**, if every element of B equals $f(a)$ for some $a \in A$. Consequently, any matrix representing an onto function has each column sum at least one, and thus $m \geq n$. In terms of bipartite graphs, for an onto function, every element of the codomain has at least one edge leading to it.

As an example, consider again the function L from all English words to the set of letters of the alphabet defined by the rule $L(w)$ is the last letter of the word w . This function is not one-to-one since, for example, $L(cat) = L(mutt)$, so two different members of the domain of L are associated with the same member (namely t) of the codomain. However, L is onto. We could prove that by making a list of twenty-six words, one ending with a , one ending with b , $\dots$, one ending with z . (Only the letters j and q might take more than a moment's thought.)

A function $f: A \rightarrow B$ which is both one-to-one and onto is called **bijective**. In the matrix of a bijection, every column has exactly one 1 and every row has exactly one 1. So, the number of rows must equal the number of columns. In other words, if there is a bijection $f: A \rightarrow B$, where A is a finite set, then A and B have the same number of elements. In such a case we will say the sets have the same **cardinality** or that they are **equinumerous**, and write that as $|A| = |B|$. The general definition (whether A and B are finite or not) is:

Definition 11.5. A and B are *equinumerous* provided there exists a bijection from A to B .

Notice that for finite sets with the same number of elements, A, B , any one-to-one function must be onto and vice versa. This is not true for infinite sets. For example, the function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ by $f(m) = 2m$ is one-to-one, but not onto, since $f(n) = 1$ is impossible for any n . On the other hand, the function $g: \mathbb{Z} \rightarrow \mathbb{Z}$ given by the rule $g(n)$ is the smallest integer that is greater than or equal to $n/2$ is onto, but not one-to-one. As examples $g(6) = 2$ and $g(-5) = -2$. This function is onto since clearly $g(2n) = n$ for any integer n , so every element of the codomain has at least one edge leading to it. But $g(1) = g(2) = 1$, so g is not one-to-one.

Since functions are relations, the **composition** of a function $g: A \rightarrow B$ by a function $f: B \rightarrow C$, makes sense. As usual, this is written as $f \circ g: A \rightarrow C$, but that's a little presumptive since it seems to assume that $f \circ g$ really is a function.

Theorem 11.6. *If $g: A \rightarrow B$ and $f: B \rightarrow C$ are functions, then $f \circ g$ is a function.*

Proof. We must show that for each $a \in A$ there is exactly one $c \in C$ so that $(a, c) \in f \circ g$. So, suppose $a \in A$. since $g: A \rightarrow B$, there is some $b \in B$ with $(a, b) \in g$. Since $f: B \rightarrow C$, there is a $c \in C$ such that $(b, c) \in f$. So, by the definition of composition, $(a, c) \in f \circ g$. That proves there is at least one $c \in C$ with $(a, c) \in f \circ g$. To complete the proof, we need to show that there is only one element of C that $f \circ g$ pairs up with a . So, suppose that

(a, c) and (a, d) are both in $f \circ g$. We need to show $c = d$. Since (a, c) and (a, d) are both in $f \circ g$, there must be elements $s, t \in B$ such that $(a, s) \in g$ and $(s, c) \in f$, and also $(a, t) \in g$ and $(t, d) \in f$. Now, since g is a function, and both (a, s) and (a, t) are in g , we can conclude $s = t$. So when we write $(t, d) \in f$, we might as well write $(s, d) \in f$. So, we know (s, c) and (s, d) are both in f . As f is a function, we can conclude $c = d$. ■

If $g: A \rightarrow B$ and $f: B \rightarrow C$, and $(a, b) \in g$ and $(b, c) \in f$, then $(a, c) \in f \circ g$. Another way to write that is $g(a) = b$ and $f(b) = c$. So $c = f(b) = f(g(a))$. That last expression looks like the familiar formula for the composition of functions found in algebra texts:

$$(f \circ g)(x) = f(g(x)).$$

When $f: A \rightarrow B$ is a function, we can form the relation f^{-1} from B to A . But f^{-1} might not be a function. For example, suppose $f: \{a, b\} \rightarrow \{1, 2\}$ is given by $f = \{(a, 1), (b, 1)\}$. Then the inverse relation $f^{-1} = \{(1, a), (1, b)\}$ is definitely not a function.

If in fact f^{-1} is a function, then for all $a \in A$ with $b = f(a)$, we have $f^{-1}(b) = a$ so

$$f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a, \forall a \in A.$$

Similarly $(f \circ f^{-1})(b) = b, \forall b \in B$. In this case we say f is **invertible**. Another way to say the same thing: the inverse of a function $f: A \rightarrow B$ is a function $g: B \rightarrow A$ which undoes the operation of f . As a particular example, consider the function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by the formula $f(n) = n + 3$. In words, f is the **add 3** function. The operation which undoes the effect of f is clearly the **subtract 3** function. That is, $f^{-1}(n) = n - 3$.

For any set S define $1_S: S \rightarrow S$ by $1_S(x) = x$ for every $x \in S$. That is $1_S = \{(x, x) | x \in S\}$. The function 1_S is called the **identity function on S** . So, the computations show $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$.

Theorem 11.7. *A function $f: A \rightarrow B$ is invertible if and only if f is bijective.*

Proof. First suppose that $f: A \rightarrow B$ is invertible. Then $f^{-1}: B \rightarrow A$ exists. If $f(a_1) = f(a_2)$, then since f^{-1} is a function, $a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2$. Thus f is one-to-one. Also if $b \in B$ with $f^{-1}(b) = a$, then $f(a) = f(f^{-1}(b)) = b$. So f is onto. Since f is one-to-one and onto, f is bijective.

Now suppose that f is bijective and let $b \in B$. Since f is onto, we have some $a \in A$ with $f(a) = b$. If $e \in A$ with $f(e) = b$, then $e = a$ since f is one-to-one. Thus b is the first entry in exactly one ordered pair in the inverse relation f^{-1} . Whence, f^{-1} is a function. ■

Do not make the error of confusing inverses and reciprocals when dealing with functions. The **reciprocal** of $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by the formula $f(n) = n + 3$ is $1/f(n) = 1/(n + 3)$ which is not the inverse function for f . For example, $f(0) = 3$, but the reciprocal of f does not convert 3 back into 0, instead the reciprocal associates 1/6 with 3.

In fact, there are other problems with the reciprocal: it doesn't even make sense when $n = -3$ since that would give a division by 0, which is undefined. So, be very careful when working with functions not to confuse the words reciprocal and inverse. They are entirely different things.

The characteristic vector (see chapter [6](#)) of a set may be used to define a special 0 – 1 function representing the given set.

Example 11.8. *Let $\mathcal{U}$ be a finite universal set with n elements ordered $u_1, \dots, u_n$. Let B_n denote all binary strings of length n . The characteristic function $\chi: P(\mathcal{U}) \rightarrow B_n$, which takes a subset A to its characteristic vector is bijective. Thus, there is no danger of miscalculation. We can either manipulate subsets of $\mathcal{U}$ using set operations and then represent the result as a binary vector or we can represent the subsets as binary vectors and manipulate the vectors with appropriate bit string operations. We'll get exactly the same answer either way.*

The process in example [11.8](#) allows us therefore to translate any set theory problem with finite sets into the world of 0's and 1's. This is the essence of computer science.

Exercises

Exercise 11.1. Recall that $\mathbb{R}$ is the set of all real numbers. In each case, give an example of a function $f: \mathbb{R} \rightarrow \mathbb{R}$ with the indicated properties, or explain why no such function exists.

- (a) f is bijective, but f is not the identity function $f(x) = x$.
- (b) f is neither one-to-one nor onto.
- (c) f is one-to-one, but not onto.
- (d) f is onto, but not one-to-one.

Exercise 11.2. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{a, b, c, d, e, f\}$. In each case, give an example of a function $f: A \rightarrow B$ with the indicated properties, or explain why no such function exists.

- (a) $f: A \rightarrow B$, f is one-to-one.
- (b) $g: B \rightarrow A$, g is one-to-one.
- (c) $f: A \rightarrow B$, f is onto.
- (d) $g: B \rightarrow A$, g is onto.

Exercise 11.3. Prove or give a counterexample: If E is an equivalence relation on a set A , then $E \circ E$ is an equivalence relation on A .

Exercise 11.4. Suppose that $g: A \rightarrow B$ and $f: B \rightarrow C$ are both one-to-one. Prove $f \circ g$ is one-to-one.

Problems

Problem 11.1. Let $A = \{1, 2, 3, 4, 5, 6\}$. In each case, give an example of a function $f: A \rightarrow A$ with the indicated properties, or explain why no such function exists.

- (a) f is bijective, but is not the identity function $f(x) = x$.
- (b) f is neither one-to-one nor onto.
- (c) f is one-to-one, but not onto.
- (d) f is onto, but not one-to-one.

Problem 11.2. Repeat problem [11.1](#) with the set $A = \mathbb{N}$.

Problem 11.3. Repeat problem [11.1](#) with the set $A = \mathbb{Z}$.

Chapter 12: Special Functions

Certain functions arise frequently in discrete mathematics. Here is a catalog of some important ones.

To begin with, the **floor function** is a function from $\mathbb{R}$ to $\mathbb{Z}$ which assigns to each real number x , the largest integer which is less than or equal to x . We denote the floor function by $\lfloor x \rfloor$. Which is to say $\lfloor x \rfloor = n$ means $n \in \mathbb{Z}$ and $n \leq x < n + 1$. For example, $\lfloor 4.2 \rfloor = 4$, and $\lfloor 7 \rfloor = 7$. Notice that for any integer n , $\lfloor n \rfloor = n$. Be a little careful with negatives: $\lfloor \pi \rfloor = 3$, but $\lfloor -\pi \rfloor = -4$. A dual function is denoted $\lceil x \rceil$, where $\lceil x \rceil = n$ means $n \in \mathbb{Z}$ and $n \geq x > n - 1$. This is the **ceiling function**. For example, $\lceil 4.2 \rceil = 5$ and $\lceil -4.2 \rceil = -4$.

The graph (in the college algebra sense!) of the floor function appears in figure [12.1](#).

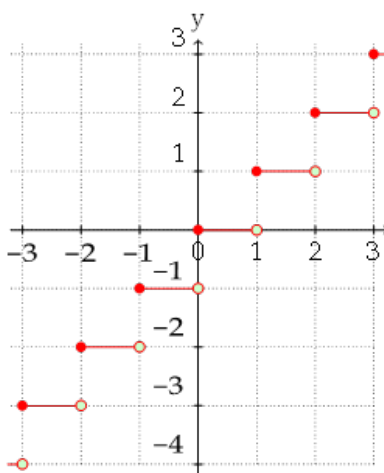


Figure 12.1: The Floor Function $y = \lfloor x \rfloor$.

The **fractional part** of a number $x \geq 0$ is denoted $\text{frac}(x)$ and equals $x - \lfloor x \rfloor$. When $x \geq 0$, the fractional part of x is just what would be expected: the stuff following the decimal point.

The definition above is the Mathematica and Wolfram/Alpha definition of the fractional part. The Graham definition extends the domain: $\text{frac}(x) = x - \lfloor x \rfloor$, for all x .

For example, $\text{frac}(5.2) = 5.2 - \lfloor 5.2 \rfloor = 5.2 - 5 = 0.2$. When x is negative its fractional part is defined to be $\text{frac}(x) = x - \lfloor x \rfloor$. Hence, we have

$$\text{frac}(x) = \begin{cases} x - \lfloor x \rfloor, & x \geq 0, \\ x - \lfloor x \rfloor, & x < 0. \end{cases}$$

For example, $\text{frac}(-5.2) = -5.2 - \lfloor -5.2 \rfloor = -5.2 - (-5) = -0.2$. In plain English, to determine the fractional part of a number x , take the stuff after the decimal point and keep the sign of the number. The graph of the fractional part function is shown in figure [12.2](#).

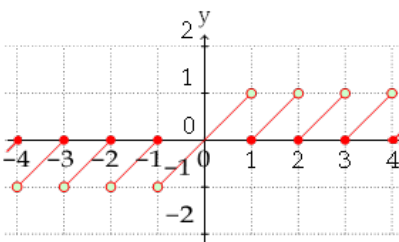


Figure 12.2: The fractional part function $y = \text{frac}(x)$.

For any real number x its **integral part** is defined to be $x - \text{frac}(x)$.

The integral part can equivalently be defined by

$$[x] = \begin{cases} \lfloor x \rfloor, & x \geq 0, \\ \lceil x \rceil, & x < 0. \end{cases}$$

The integral part of x is denoted by $[x]$, or, sometimes, by $\text{int}(x)$. In words, the integral part of x is found by discarding everything following the decimal (at least if we agree not to end decimals with an infinite string of 9's such as $2.9999\dots$). The graph of the integral part function is displayed in figure [12.3](#).

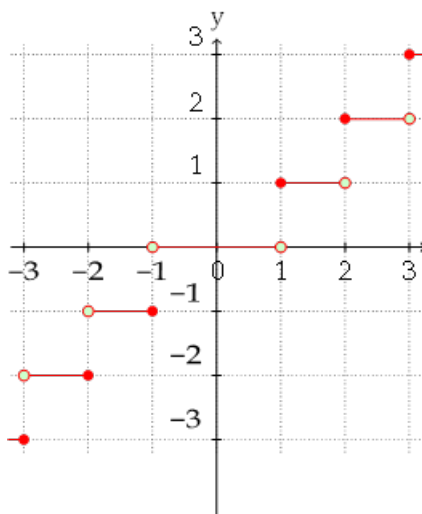


Figure 12.3: The integral part function $y = [x]$.

The **power functions** are familiar from college algebra. They are the functions of the form $f(x) = x^2$, $f(x) = x^3$, $f(x) = x^4$ and so on. By extension, $f(x) = x^a$, where a is any constant greater than or equal to 1 will be called a power function.

For any set X , the unit power function $1_X(x) = x$ for all $x \in X$ is called the **identity** function.

Exchanging the roles of the variable and the constant in the power functions leads to a whole class of nice functions, those of the form $f: \mathbb{R} \rightarrow \mathbb{R}$, where $f(x) = a^x$, and $0 < a$. Such a function f is called the **base a exponential function**. The function is uninteresting when $a = 1$. Also, if $0 < b < 1$, then the function $g(x) = b^x = 1/f(x)$, where $f(x) = a^x$ and $a = 1/b > 1$. So we may focus on $a > 1$. In fact, the most important values for a are 2, e and 10.

The number $e \approx 2.718281828459\dots$ is called the **natural base**, but that story belongs to calculus. Base 2 is the usual base for computer science. Engineers are most interested in base 10, while mathematicians often use the natural exponential function, e^x .

By graphing the function $f: \mathbb{R} \rightarrow (0, \infty)$ defined by $y = f(x) = e^x$ we can see that it is bijective. We denote the inverse function $f^{-1}(x)$ by $\ln x$ and call it the **natural log function**. Since these are inverse functions we have

$$e^{\ln a} = a, \forall a > 0 \text{ and } \ln(e^b) = b, \forall b \in \mathbb{R}.$$

As a consequence $a^x = (e^{\ln a})^x = e^{(\ln a) \cdot x} = e^{x \ln a}$ is determined as the composition of the function $y = \ln(a) \cdot x$ by the natural exponential function. So, every exponential function is invertible with inverse denoted as $\log_a x$, the **base a logarithmic function**. Besides the natural log, $\ln x$, we often write $\lg x$ for the base 2 logarithmic function, and $\log x$ with no subscript to denote the base 10 logarithmic function.

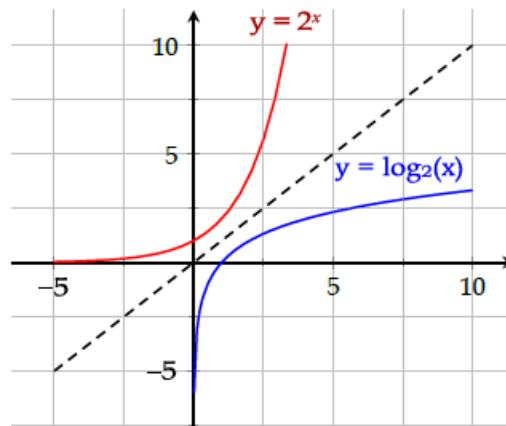


Figure 12.4: Graphs of the functions $y = 2^x$ and $y = \lg x$.

The basic facts needed for manipulating exponential and logarithmic functions are the laws of exponents.

Theorem 12.1 (Laws of Exponents). For $a, b, c \in \mathbb{R}$, $a^{b+c} = a^b a^c$ and $a^c b^c = (ab)^c$.

From the laws of exponents, we can derive the

Theorem 12.2 (Laws of Logarithms). For $a, b, c > 0$, $\log_a bc = \log_a b + \log_a c$, and $\log_a(b^c) = c \log_a b$.

Proof. We rely on the fact that all exponential and logarithmic functions are one-to-one. Hence, we have that $a^{\log_a bc} = bc = a^{\log_a b} a^{\log_a c} = a^{\log_a b + \log_a c}$ implies $\log_a bc = \log_a b + \log_a c$.

Similarly, the second identity follows from $a^{\log_a b^c} = b^c = (a^{\log_a b})^c = a^{c(\log_a b)}$. ■

Notice that $\log_a(1/b) = \log_a(b^{-1}) = -\log_a b$.

Calculators typically have buttons for logs base e and base 10. If $\log_a b$ is needed for a base different from e and 10, it can be computed in a roundabout way. Suppose we need to find the value $c = \log_a b$. In other words, we need the number c such that $a^c = b$. Taking the natural log of both sides of that equation we get

$$a^c = b$$

$$\ln a^c = \ln b$$

$$c \ln a = \ln b$$

$$c = \frac{\ln b}{\ln a}$$

Hence, we have the general relation between logarithms as follows.

Corollary 12.3. $\log_a x = \ln x / \ln a$.

Example 12.4. *For example, we see that $\log_2 100 = \ln 100 / \ln 2 \approx 6.643856$.*

Exercises

Exercise 12.1. *In words, $\lfloor x \rfloor$ is the largest integer less than or equal to x . Complete the sentence: In words, $\lceil x \rceil$ is the smallest ...*

Exercise 12.2. *Draw a (college algebra) graph of $f(x) = \lfloor x \rfloor$.*

Exercise 12.3. *Draw a (college algebra) graph of $f(x) = \lfloor 2x - 1 \rfloor$.*

Exercise 12.4. *Draw a (college algebra) graph of $f(x) = 2\lfloor x - 1 \rfloor$.*

Exercise 12.5. *Let $f(x) = 18x$ and let $g(x) = x^3/2$. Sketch the graphs of f, g for $x \geq 1$ on the same set of axes. Notice that the graph g is lower than the graph of f when $x = 1$, but it is above the graph of f when $x = 9$. Where does g cross the graph of f (in other words, where does g catch up with f)?*

Exercise 12.6. *Let $f(x) = 4x^5$ and let $g(x) = 2^x$. For values of $x \geq 1$ it appears that the graph of g is lower than the graph of f . Does g ever catch up with f , or does f always stay ahead?*

Exercise 12.7. *The x^y button on your calculator is broken. Show how you can approximate $2^{\sqrt{2}}$ with your calculator anyhow.*

Problems

Problem 12.1. *Write $(52) \ln 5 - 4 \ln 3$ as a single logarithm.*

Problem 12.2. *Draw the college algebra style graph of $f(x) = e^{x+3} - 1$.*

Problem 12.3. *Let $f(x) = 2x^3$ and $g(x) = 3^x$. Notice that $f(1) < g(1)$ and $f(2) > g(2)$. Does g ever catch up with f again, or does f always stay ahead of g ?*

Problem 12.4. *Write $\log 1 + \log 2 + \log 3 + \log 4 + \log 5 + \log 6$ as a single logarithm.*

Problem 12.5. *Write $\sum_{k=1}^n \log k$ as a single logarithm.*

Chapter 13: Sequences and Summations

A **sequence** is a list of numbers in a specific order. For example, the positive integers $1, 2, 3, \dots$ is a sequence, as is the list $4, 3, 3, 5, 4, 4, 3, 5, 5, 4$ of the number of letters in the English words of the ten digits in order *zero, one, ... , nine*. Actually, the first is an example of an infinite sequence, the second is a finite sequence. The first sequence goes on forever; there is no last number. The second sequence eventually comes to a stop. In fact, the second sequence has only ten items. A **term** of a sequence is one of the numbers that appears in the sequence. The first term is the first number in the list, the second term is the second number in the list, and so on.

A more general way to think of a sequence is as a function from some subset of $\mathbb{Z}$ having a least member (in most cases either $\{0, 1, 2, \dots\}$ or $\{1, 2, \dots\}$) with codomain some *arbitrary* set.

Computer science texts use the former and elementary math application texts use the later. Mathematicians use any such well-ordered domain set.

In most mathematics courses the codomain will be a set of numbers, but that isn't necessary. For example, consider the finite sequence of initial letters of the words in the previous paragraph: $a, s, i, a, l, o, n, \dots, a, s, o$. If the letter L is used to denote the function that forms this sequence, then $L(1) = a, L(2) = s$, and so on.

The examples of sequences given so far were described in words, but there are other ways to tell what objects appear in the sequence. One way is with a formula. For example, let $s(n) = n^2$, for $n = 1, 2, 3, \dots$. As the values $1, 2, 3$ and so on are plugged into $s(n)$ in succession, the infinite sequence $1, 4, 9, 16, 25, 36, \dots$ is built up. It is traditional to write s_n (or t_n , etc) instead of $s(n)$ when describing the terms of a sequence, so the formula above would usually be seen as $s_n = n^2$. Read that as *s sub n equals n squared*. When written this way, the n in the s_n is called a *subscript* or *index*. The subscript of s_{173} is 173.

Example 13.1. What is the 50th term of the sequence defined by $s_j = \frac{j+1}{j+2}$, where $j = 1, 2, 3, \dots$?
We see that

$$s_{50} = \frac{51}{52}.$$

Example 13.2. What is the 50th term of the sequence defined by $t_k = \frac{k+1}{k+2}$, where $k = 0, 1, 2, \dots$?
We see that

$$t_{49} = \frac{50}{51}.$$

A sequence can also be specified by listing an initial portion of the sequence and trust the reader to successfully perform the mind reading trick of guessing how the sequence is to continue based on the pattern suggested by those initial terms. For example, consider the sequence $7, 10, 13, 16, 19, 22, \dots$. The symbol $\dots$ means *and so on*. In other words, you *should* be able to figure out the way the sequence will continue. This method of specifying a sequence is dangerous of course. For instance, the number of terms sufficient for one person to spot the pattern might not be

enough for another person. Also, maybe there are several different *obvious* ways to continue the pattern.

Example 13.3. *What is the next term in the sequence 1, 3, 5, 7 ...? One possible answer is 9, since it looks like we are listing the positive odd integers in increasing order. But another possible answer is 8: maybe we are listing each positive integer with an *e* in its name. You can probably think of other ways to continue the sequence.*

In fact, for any finite list of initial terms, there are always infinitely many more or less natural ways to continue the sequence. A reason can always be provided for absolutely any number to be the next in the sequence. However, there will typically be only one or two *obvious* simple choices for continuing a sequence after five or six terms.

The simple pattern suggested by the initial terms 7, 10, 13, 16, 19, 22, ... is that the sequence begins with a 7, and each term is produced by adding 3 to the previous term. This is an important type of sequence. The general form is $s_1 = a$ (a is just some specific number), and, from the second term on, each new term is produced by adding d to the previous term (where d is some fixed number).

In the last example, $a = 7$ and $d = 3$. A sequence of this form is called an **arithmetic sequence**. The number d is called the **common difference**, which makes sense since d is the difference of any two consecutive terms of the sequence. It is possible to write down a formula for s_n in this case. After all, to compute s_n we start with the number a , and begin adding d 's to it. Adding one d gives $s_2 = a + d$, adding two d 's gives $s_3 = a + 2d$, and so on. For s_n we will add $n - 1$ d 's to the a , and so we see $s_n = a + (n - 1)d$. In the numerical example above, the 5th term of the sequence ought to be $s_5 = 7 + 4 \cdot 3 = 19$, and sure enough it is. The 407th term of the sequence is $s_{407} = 7 + 406 \cdot 3 = 1225$.

Example 13.4. *The 1st term of an arithmetic sequence is 11 and the 8th term is 81. What is a formula for the n^{th} term?*

We know $a_1 = 11$ and $a_8 = 81$. Since $a_8 = a_1 + 7d$, where d is the common difference, we get the equation $81 = 11 + 7d$. So $d = 10$. We can now write down a formula for the terms of this sequence: $a_n = 11 + (n - 1)10 = 1 + 10n$. Checking, we see this formula does give the required values for a_1 and a_8 .

For an arithmetic sequence we added the same quantity to get from one term of the sequence to the next. If instead of adding we multiply each term by the same thing to produce the next term the result is called a **geometric sequence**.

Example 13.5. *Let $s_1 = 2$, and suppose we multiply by 3 to get from one term to the next. The sequence we build now looks like 2, 6, 18, 54, 162, $\dots$, each term being 3 times as large as the previous term.*

In general, if $s_1 = a$, and for $n \geq 1$ each new term is r times the preceding term, then the formula for the n^{th} term of the sequence is $s_n = ar^{n-1}$, which is reasoned out just as for the formula for the arithmetic sequence above. The quantity r in the geometric sequence is called the

common ratio since it is the ratio of any term in the sequence to its predecessor (assuming $r \neq 0$ at any rate).

A sequence of numbers is an ordered list of numbers. A **summation** (or just **sum**) is a sequence of numbers added up. A sum with n terms (that is, with n numbers added up) will be denoted by S_n typically. If we are dealing with sequence $1, 3, 5, 7, \dots, 2n - 1, \dots$, then $S_3 = 1 + 3 + 5$, and $S_n = 1 + 3 + 5 + \dots + (2n - 1)$. For the arithmetic sequence $a, a + d, a + 2d, a + 3d, \dots$, we see $S_n = a + (a + d) + (a + 2d) + \dots + (a + (n - 1)d)$.

It gets a little awkward writing out such extended sums and so a compact way to indicate a sum, called **summation notation**, is introduced. For the sum of the first 3 odd positive integers above we would write $\sum_{j=1}^3 (2j - 1)$. The Greek letter sigma (Σ) is supposed to be reminiscent of the word summation. The j is called the **index of summation** and the number on the bottom of the Σ specifies the starting value of j while the number above the Σ gives the ending value of j . The idea is that we replace j in turn by 1, 2 and 3, in each case computing the value of the expression following the Σ , and then add up the terms produced. In this example, when $j = 1, 2j - 1 = 1$, when $j = 2, 2j - 1 = 3$ and finally, when $j = 3, 2j - 1 = 5$. We've reached the stopping value, so we have $\sum_{j=1}^3 (2j - 1) = 1 + 3 + 5 = 9$.

Notice that the index of summation takes only integer values. If it starts at 6, then next it is replaced by 7, and so on. If it starts at -11 , then next it is replaced by -10 , and then by -9 , and so on.

The symbol used for the index of summation does not have to be j . Other traditional choices for the index of summation are i, k, m and n . So for example,

$$\sum_{j=0}^4 (j^2 + 2) = 2 + 3 + 6 + 11 + 18 = \sum_{i=0}^4 (i^2 + 2) = \sum_{m=0}^4 (m^2 + 2)$$

and so on. Even though a different index letter is used, the formulas produce the same sequence of numbers to be added up in each case, so the sums are the same.

Also, the starting and ending points can for the index can be changed without changing the value of the sum provided care is taken to change the formula appropriately. Notice that

$$\sum_{k=1}^3 (3k - 1) = \sum_{k=0}^2 (3k + 2).$$

In fact, if the terms are written out we see that both sums represent $2 + 5 + 8 = 15$.

Example 13.6. *We see that*

$$\sum_{m=-1}^5 2^m = 2^{-1} + 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = \frac{127}{2}.$$

Example 13.7. *We find that*

$$\sum_{n=3}^6 2 = 2 + 2 + 2 + 2 = 8.$$

There are two important formulas for finding sums that are worth remembering. The first is the sum of the first n terms of an arithmetic sequence.

$$S_n = a + (a + d) + (a + 2d) + \cdots + (a + (n - 1)d).$$

Here is a clever trick that can be used to find a simple formula for the quantity S_n : the list of numbers is added up twice, once from left to right, the second time from right to left. When the terms are paired up, it is clear the sum is $2S_n = n[a + (a + (n - 1)d)]$. A diagram will make the idea clearer:

$$\begin{array}{ccccccc} a & & + (a + d) & & + (a + 2d) & & + \cdots (a + (n - 1)d) \\ + (a + (n - 1)d) & + (a + (n - 2)d) & + (a + (n - 3)d) & + \cdots & + a & & \\ \hline (2a + (n - 1)d) & + (2a + (n - 1)d) & + (2a + (n - 1)d) & + \cdots & + (2a + (n - 1)d) & & \end{array}$$

The bottom row contains n terms, each equal to $2a + (n - 1)d$ so $2S_n = n[2a + (n - 1)d]$. Dividing by 2 gives the important formula for $n = 1, 2, 3, \dots$,

$$S_n = n \left(\frac{2a + (n - 1)d}{2} \right) = n \left(\frac{a + (a + (n - 1)d)}{2} \right)$$

Equation 13.1

An easy way to remember the formula is to think of the quantity in the parentheses as the average of the first and last terms to be added, and the coefficient, n , as the number of terms to be added.

Example 13.8. *The sum of the first 20 terms of the arithmetic sequence 5, 9, 13, $\dots$ is found to be*

$$s_{20} = 20 \left(\frac{5 + 81}{2} \right) = 860.$$

For a geometric sequence a little algebra produces a formula for the sum of the first n terms of the sequence. The resulting formula for $S_n = a + ar + ar^2 + \cdots + ar^{n-1}$ is

$$S_n = \frac{a - ar^n}{1 - r} = a \left(\frac{1 - r^n}{1 - r} \right), \text{ if } r \neq 1.$$

Example 13.9. *The sum of the first ten terms of the geometric sequence $2, \frac{2}{3}, \frac{2}{9}, \dots$ would be*

$$S_{10} = \frac{2 - 2 \left(\frac{1}{3} \right)^{10}}{1 - \left(\frac{1}{3} \right)}.$$

The expression for S_{10} can be simplified as

$$S_{10} = \frac{2 - 2\left(\frac{1}{3}\right)^{10}}{1 - \left(\frac{1}{3}\right)} = 2 \left(\frac{1 - \left(\frac{1}{3}\right)^{10}}{1 - \left(\frac{1}{3}\right)} \right) = 2 \left(\frac{1 - \left(\frac{1}{3}\right)^{10}}{\frac{2}{3}} \right) = 3 \left(1 - \frac{1}{3^{10}} \right) = 3 - \frac{1}{3^9}.$$

Notice that the numerator in this case is the difference of the first term we have to add in and the term immediately following the last term we have to add in.

Here is the algebra that shows the geometric sum formula is correct.

Let $S_n = a + ar + ar^2 + \cdots + ar^{n-1}$. Multiply both sides of that equation by r to get

$$rS_n = r(a + ar + ar^2 + \cdots + ar^{n-1}) = ar + ar^2 + ar^3 + \cdots + ar^{n-1} + ar^n.$$

Now subtract, and observe that most terms will cancel:

$$\begin{aligned} S_n - rS_n &= (a + ar + ar^2 + \cdots + ar^{n-1}) - (ar + ar^2 + ar^3 + \cdots + ar^{n-1} + ar^n) \\ &= a + (ar + ar^2 + ar^3 + \cdots + ar^{n-1}) - (ar + ar^2 + ar^3 + \cdots + ar^{n-1}) - ar^n \\ &= a - ar^n \end{aligned}$$

So $S_n(1 - r) = a - ar^n$. Assuming $r \neq 1$, we can divide both sides of that equation by $1 - r$, producing the promised formula:

$$S_n = \frac{a - ar^n}{1 - r} = a \left(\frac{1 - r^n}{1 - r} \right), \text{ if } r \neq 1.$$

13.2: The sum formula for geometric sequences

You should be able to find a formula for S_n when $r = 1$.

Exercises

Exercise 13.1. Guess the next term in the sequence 1,2,4,5,7,8, What's another possible answer?

Exercise 13.2. What is the 100th term of the arithmetic sequence with initial term 2 and common difference 6?

Exercise 13.3. The 10th term of an arithmetic sequence is -4 and the 16th term is 47. What is the 11th term?

Exercise 13.4. What is the 5th term of the geometric sequence with initial term 6 and common ratio 2?

Exercise 13.5. The first two terms of a geometric sequence are $g_1 = 5$ and $g_2 = -11$. What is g_5 ?

Exercise 13.6. Which sequences are both a geometric sequence and also an arithmetic sequence?

Exercise 13.7. Evaluate $\sum_{j=1}^4 (j^2 + 1)$.

Exercise 13.8. Evaluate $\sum_{k=-2}^4 (2k - 3)$.

Exercise 13.9. What is the sum of the first 100 terms of the arithmetic sequence with initial term 2 and common difference 6?

Exercise 13.10. What is the sum of the first five terms of the geometric sequence with initial term 6 and common ratio 2?

Exercise 13.11. Evaluate $\sum_{i=0}^4 \left(-\frac{3}{2}\right)^i$.

Exercise 13.12. Express in summation notation: $\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots + \frac{1}{2n}$ the sum of the reciprocals of the first n positive even integers.

Problems

Problem 13.1. *Guess the next term in the sequence 1, 3, 5, 7, 8, 9 · · · . What's another possible answer?*

Problem 13.2. *Guess the next term in the sequence 1, 2, 2, 3, 2, 4, 2, 4, 3 · · · .*

Problem 13.3. *A sequence begins 1, 3, 9, 15. Could it be an arithmetic sequence? Could it be a geometric sequence?*

Problem 13.4. *What is the 20th term of the arithmetic sequence with initial term 4 and common difference 5?*

Problem 13.5. *The 8th term of an arithmetic sequence is 20 and the 12th term is 40. What is the 25th term?*

Problem 13.6. *What is the 7th term of the geometric sequence with initial term 3 and common ratio 4?*

Problem 13.7. *Two terms of a geometric sequence are $g_3 = 2$ and $g_5 = 72$. There are two possible values for g_4 . What are those two values?*

Problem 13.8. *A geometric sequence has initial term 3, and common ratio 7. Determine the smallest value of n so that the n^{th} term of the sequence is more than one million.*

Problem 13.9. *Evaluate $\sum_{j=1}^4 (j + 1)^2$.*

Problem 13.10. *Evaluate $\sum_{k=-2}^4 (2k + 3)$.*

Problem 13.11. *What is the sum of the first 100 terms of the arithmetic sequence with initial term 2 and common difference 6?*

Problem 13.12. *What is the sum of the first four terms of the geometric sequence with initial term 3 and common ratio -2 ?*

Problem 13.13. *What is the sum of the first four thousand terms of the geometric sequence with initial term 3 and common ratio -1 ?*

Problem 13.14. *Evaluate $\sum_{i=0}^4 \left(\frac{3}{2}\right)^i$.*

Problem 13.15. *Express in summation notation: $\frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$ is the sum of the reciprocals of the first n odd integers.*

PART III: Recursion, Induction and Algorithms

Chapter 14: Recursively Defined Sequences

Besides specifying the terms of a sequence with a formula, such as $a_n = n^2$, an alternative is to give an initial term, usually something like b_1 , (or the first few terms, $b_1, b_2, b_3 \dots$) of a sequence, and then give a rule for building new terms from old ones. In this case, we say the sequence has been defined **recursively**.

Example 14.1. For example, suppose $b_1 = 1$, and for $n > 1$, $b_n = 2b_{n-1}$. Then the 1st term of the sequence will be $b_1 = 1$ of course. To determine b_2 , we apply the rule $b_2 = 2b_{2-1} = 2b_1 = 2 \cdot 1 = 2$. Applying the rule again, $b_3 = 2b_{3-1} = 2b_2 = 2 \cdot 2 = 4$. Next $b_4 = 2b_3 = 8$. Continuing in this fashion, we can form as many terms of the sequence as we wish: 1, 2, 4, 8, 16, 32, $\dots$. Here it is easy to guess a formula for the terms of the sequence: $b_n = 2^{n-1}$.

In general, to define a sequence recursively, (1) we first give one or more initial terms (this information is called the **initial condition(s)** for the sequence), and then (2) we give a rule for forming new terms from previous terms (this rule is called the **recursive formula**).

Example 14.2. Consider the sequence defined recursively by $a_1 = 0$, and, for $n \geq 2$,

$$a_n = 2a_{n-1} + 1.$$

The five terms of this sequence are $0, 2 \cdot 0 + 1 = 1, 2 \cdot 1 + 1 = 3, 2 \cdot 3 + 1 = 7, 2 \cdot 7 + 1 = 15$. In words, we can describe this sequence by saying the initial term is 0 and each new term is one more than twice the previous term. Again, it is easy to guess a formula that produces the terms of this sequence: $a_n = 2^{n-1} - 1$ for $n \geq 1$.

Such a formula for the terms of a sequence is called a **closed form formula** to distinguish it from a recursive formula.

There is one big advantage to knowing a closed form formula for a sequence. In example [14.2](#) above, the closed form formula for the sequence tells us immediately that $a_{101} = 2^{100} - 1$, but using the recursive formula to calculate a_{101} means we have to calculate in turn $a_1, a_2, \dots, a_{100}$, making 100 computations. The closed form formula allows us to jump directly to the term we are interested in. The recursive formula forces us to compute 99 additional terms we don't care about in order to get to the one we want. With such a major drawback why even introduce recursively defined sequences at all? The answer is that there are many naturally occurring sequences that have simple recursive definitions but have no reasonable closed form formula, or even no closed form formula at all in terms of familiar operations. In such cases, a recursive definition is better than nothing.

There are methods for determining closed form formulas for some special types of recursively defined sequences. Such techniques are studied later in chapter [35](#). For now, we are only interested in understanding recursive definitions, and determining some closed form formulas by the method of *pattern recognition* (aka guessing).

The most famous recursively defined sequence is due to Fibonacci. There are two initial conditions: $f_0 = 0$ and $f_1 = 1$. The index starts at **zero**, by tradition. The recursive rule is, for

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

In words, each new term is the sum of the two terms that precede it. So, the **Fibonacci sequence** begins

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots$$

There is a closed form formula for the Fibonacci Sequence, but it is not at all easy to guess:

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n, n \geq 0.$$

For a positive integer n , the symbol $n!$ is read **n factorial** and it is defined to be the product of all the positive integers from 1 to n . For example, $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. In order to make many formulas work out nicely, the value of $0!$ is defined to be 1.

A recursive formula can be given for $n!$. The initial term is $0! = 1$, and the recursive rule is,

$$n! = n[(n - 1)!], \text{ for } n \geq 1.$$

Hence, the first few factorial values are:

$$1! = 1[0!] = 1 \cdot 1 = 1,$$

$$2! = 2[1!] = 2 \cdot 1 = 2,$$

$$3! = 3[2!] = 3 \cdot 2 = 6,$$

$$4! = 4[3!] = 4 \cdot 6 = 24.$$

We sometimes write a *general* formula for the factorial as

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n, \text{ for } n > 0.$$

The sequence of factorials grows very quickly. Here are the first few terms:

$$1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, 39916800, 479001600, 6227020800, \dots$$

Consider the terms of an arithmetic sequence with initial term a and common difference d :

$$a, (a + d), (a + 2d), \dots, (a + (n - 1)d), \dots$$

These terms may clearly be found by adding d to the current term to get the next. That is, the arithmetic sequence may be defined recursively as (1) $a_1 = a$, and (2) for $n \geq 2$, $a_n = a_{n-1} + d$.

Exercises

Exercise 14.1. List the first five terms of the sequence defined recursively by $a_1 = 3$, and the recursive formula for $n \geq 2$, $a_n = a_{n-1}(2 + a_{n-1})$.

Exercise 14.2. List the first seven terms of the sequence defined recursively by $a_0 = 1, a_1 = 1$, and for $n \geq 2$, $a_n = 1 + a_{n-1}a_{n-2}$.

Exercise 14.3. List the first ten terms of the sequence defined recursively by $a_0 = 1$, and the recursive formula, for $n \geq 1$, $a_n = 1 + a_{\lfloor n/2 \rfloor}$.

Exercise 14.4. List the first ten terms of the sequence defined recursively by $a_0 = 1$, and the recursive formula for $n \geq 1$, $a_n = 2n - a_{n-1} - 1$, and guess a closed form formula for a_n .

Exercise 14.5. The first few terms of a sequence are

$$1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211.$$

There is an easy recursive rule for building the terms of this sequence. Guess the next term.

Exercise 14.6. Let d be a fixed real number. For a positive integer n , the symbol nd means the sum of n d 's. Give a recursive definition of nd analogous to the definition of $n!$ given in this chapter.

Problems

Problem 14.1. List the first five terms of the sequence defined recursively by $a_1 = 2$, and the recursive formula, for $n \geq 2$, $a_n = a_{n-1}^2 - 1$.

Problem 14.2. List the first five terms of the sequence defined recursively by $a_1 = 2$, and the recursive formula for $n \geq 2$, $a_n = 3a_{n-1} + 2$. Guess a closed form formula. Hint: This is a lot like example [14.2](#). for the sequence.

Problem 14.3. List the first five terms of the sequence with initial terms $u_0 = 2$ and $u_1 = 5$, and, for $n \geq 2$, $u_n = 5u_{n-1} - 6u_{n-2}$. Guess a closed form formula for the sequence. Hint: The terms are simple combinations of powers of 2 and powers of 3.

Problem 14.4. Let r be a fixed real number different from 0. For a positive integer n , the symbol r^n means the product of n r 's. For convenience, r^0 is defined to be 1. Give a recursive definition of r^n analogous to the definition of $n!$ given in this chapter.

Problem 14.5. Give a recursive definition of the geometric sequence with initial term 3 and common ratio 2.

Problem 14.6. Generalize problem 14.5: give a recursive definition of the geometric sequence with initial term a and common ratio r .

Chapter 15: Recursively Defined Sets

An Ancient Song

Two different ways of defining a set have been discussed. We can describe a set by the roster method, listing all the elements that are to be members of the set, or we can describe a set using set-builder notation by giving a predicate that the elements of the set are to satisfy. Here we consider defining sets in another natural way: recursion.

Recursive definitions can also be used to build sets of objects. The spirit is the same as for recursively defined sequences: give some initial conditions and a rule for building new objects from ones already known.

Example 15.1. *For instance, here is a way to recursively define the set E of positive even integers. First, the initial condition: $2 \in E$. Next the recursive portion of the definition: If $x \in E$, then $x + 2 \in E$. Here is what we can deduce using these two rules. First of course, we see $2 \in E$ since that is the given initial condition. Next, since we know $2 \in E$, the recursive portion of the definition, with x being played by 2, says $2 + 2 \in E$, so that now we know $4 \in E$. Since $4 \in E$, the recursive portion of the definition, with x now being played by 4, says $4 + 2 \in E$, so that now we know $6 \in E$. Continuing in this way, it gets easy to believe that E really is the set of positive even integers.*

Actually, there is a little more to do with example 15.1. The claim is that E consists of exactly all the positive even integers. In other words, we also need to make sure that no other things appear in E besides the positive even integers. Could 312211 somehow have slithered into the set E ? To verify that such a thing does not happen, we need one more fact about recursively defined sets. The only elements that appear in a set defined recursively are those that make it on the basis of either the initial condition or the recursive portion of the definition. No elements of the set appear, as if by magic, from nowhere.

In this case, it is easy to see that no odd integers sneak into the set. For if so, there would be a smallest odd integer in the set and the only way it could be elected to the set is if the integer two less than it were in the set. But that would mean a yet smaller odd integer would be in the set, a contradiction. We won't go into that sort of detail for the following examples in general. We'll just consider the topic at the intuitive level only.

Example 15.2. *Give a recursive definition of the set, S , of all non-negative integer powers of 2.*

Initial condition: $1 \in S$.

Recursive rule: If $x \in S$, then $2x \in S$.

Applying the initial condition and then the recursive rule repeatedly gives the elements:

$$1, 2 \cdot 1 = 2, 2 \cdot 2 = 4, 2 \cdot 4 = 8, 2 \cdot 8 = 16$$

and so on, and that looks like the set of nonnegative powers of 2.

Example 15.3. *A set, S , is defined recursively by*

Initial conditions: $1 \in S$ and $2 \in S$.

Recursive rule: If $x \in S$, then $x + 3 \in S$. Describe the integers in S .

The plan is to use the initial conditions and the recursive rule to build elements of S until we can guess a description of the integers in S . From the initial conditions we know $1 \in S$ and $2 \in S$. Applying the recursive rule to each of those we get $4, 5 \in S$, and using the recursive rule on those gives $7, 8 \in S$, and so on.

So, we get $S = \{1, 2, 4, 5, 7, 8, 10, 11, \dots\}$ and it's apparent that S consists of the positive integers that are not multiples of 3.

Subtly, we could have started with the initial term 1 and deduced that $\{1, 4, 7, 10, \dots\} \subset S$. And then used the initial term 2 to conclude that $\{2, 5, 8, 11, \dots\} \subset S$. We then arrive at the point that $S = \{1, 4, 7, 10, \dots, 2, 5, 8, 11, \dots\}$ which of course is the same as above, just in a different order.

Recursively defined sets appear in certain computer science courses where they are used to describe sets of strings. To form a string, we begin with an **alphabet** which is a set of symbols, traditionally denoted by Σ . For example, $\Sigma = \{a, b, c\}$ is an alphabet of three symbols, whereas $\Sigma = \{!, @, \#, \$, \%, \&, X, 5\}$ is an alphabet of eight symbols. A **string** over the alphabet Σ is any finite sequence of symbols from the alphabet. For example, $aaba$ is a string of **length** four over the $\Sigma = \{a, b, c\}$, and $!!5X\$\$5@@$ is a length nine string over $\Sigma = \{!, @, \#, \$, \%, \&, X, 5\}$. There is a special string over any alphabet denoted by λ called the **empty string**. It contains no symbols and has length 0.

Example 15.4. *A set, S , of strings over the alphabet $\Sigma = \{a, b\}$ is given recursively by (1) $\lambda \in S$, and (2) If $x \in S$, then $axb \in S$. Describe the strings in S .*

The notation axb means write down the string a followed by the string x followed by the string b . So if $x = aaba$ then $axb = aaabab$. Let's experiment with the recursive rule a bit, and then guess a description for the strings in S . Starting with the initial condition we see $\lambda \in S$. Applying the recursive rule to λ gives $a\lambda b = ab \in S$. Applying the recursive rule to ab gives $aabb \in S$, and applying the recursive rule to $aabb$ shows $aaabbb \in S$. It's easy to guess the nature of the strings in S : Any finite string of a 's followed by the same number of b 's.

Stealing some notation from algebra we might write $S = \{a^k b^k \mid k \in \mathbb{N}\}$.

Example 15.5. *Give a recursive definition of the set S of strings over $\Sigma = \{a, b, c\}$ which do not contain adjacent a 's. For example, $ccabbbabba$ is acceptable, but $abcbaabaca$ is not.*

For the initial conditions we will use (1) $\lambda \in S$, and $a \in S$. If we have a string with no adjacent a 's, we can extend it by adding b or c to either end. But we'll need to be careful when adding more a 's. For the recursive rule we will use (2) if $x \in S$, then $bx, xb, cx, xc \in S$ and $abx, xba, acx, xca \in S$. Notice how the string a had to be put into S in the initial conditions since the recursive rule won't allow us to form that string from λ .

Here is different answer to the same question. It's a little harder to dream up, but the rules are much cleaner. The idea is that if we take two strings with no adjacent a 's, we can put them together and be sure to get a new string with no adjacent a 's provided we stick either b or c

between them. So, we can define the set recursively by (1) $\lambda \in S$ and $a \in S$, and (2) if $x, y \in S$, then $xby, xcy \in S$.

Example 15.6. Give a recursive definition of the set S of strings over $\Sigma = \{a, b\}$ which contain more a 's than b 's.

The idea is that we can build longer strings from smaller ones by (1) sticking two such strings together, or (2) sticking two such strings together along with a b before the first one, between the two strings, or after the last one. That leads to the following recursive definition: (1) $a \in S$ and (2) if $x, y \in S$ then $xy, bxy, xby, xyb \in S$. That looks a little weird since in the recursive rule we added b , but since x and y each have more a 's than b 's, the two together will have at least two more a 's than b 's, so it's safe to add b in the recursive rule.

Starting with the initial condition, and then applying the recursive rule repeatedly, we form the following elements of S :

$a, aa, baa, aba, aab, aaa, baaa, abaa, aaba, baaa, \dots$

Example 15.7. A set S of strings over the alphabet $\Sigma = \{a, b\}$ is defined recursively by the rules (1) $a \in S$, and (2) if $x \in S$, then $xbx \in S$. Describe the strings in S .

Experimenting we find the following elements of S :

$a, aba, abababa, abababababababa, \dots$

It looks like S is the set of strings beginning with a followed by a certain number of ba 's. If we look at the number of ba 's in each string, we can see a pattern: 0, 1, 3, 7, 15, 31, ..., which we recognize as being the numbers that are one less than the positive integer powers of 2 (1, 2, 4, 8, 16, 32, ...). So, it appears S is the set of strings which consist of a followed by $2^n - 1$ pairs ab for some integer $n \geq 0$. Using algebraic notation

$$S = \{a(ba)^k \mid k = 2^n - 1, n \in \mathbb{N}\}.$$

Exercises

Exercise 15.1. *The set S is described recursively by (1) $1 \in S$, and (2) if $n \in S$, then $n + 1 \in S$. To what familiar set is S equal?*

Exercise 15.2. *Give a recursive definition of the set of positive integers that end with the digits 17.*

Exercise 15.3. *Give a recursive definition of the set of positive integers that are not multiples of 4.*

Exercise 15.4. *Describe the strings in the set S of strings over the alphabet $\Sigma = \{a, b, c\}$ defined recursively by (1) $\lambda \in S$ and (2) if $x \in S$, then $axbc \in S$.*

Exercise 15.5. *Describe the strings in the set S of strings over the alphabet $\Sigma = \{a, b, c\}$ defined recursively by (1) $c \in S$ and (2) if $x \in S$ then $ax \in S$ and $bx \in S$ and $xc \in S$.*

Exercise 15.6. *A **palindrome** is a string that reads the same in both directions. For example, a classic palindrome with length 21 is: A man, a plan, a canal: panama. For another example, aabaa is a palindrome of length five and babccbab is a palindrome of length eight. The empty string is also a palindrome. Give a recursive definition of the set of palindromes over the alphabet $\Sigma = \{a, b, c\}$.*

Problems

Problem 15.1. A set S of integers is defined recursively by the rules (1) $1 \in S$, and (2) If $n \in S$, then $2n + 1 \in S$.

- a) Is $15 \in S$? Explain your answer.
- b) Is $65 \in S$? Explain your answer.

Problem 15.2. A set of integers is defined recursively by the rules (1) $0 \in S$, and (2) if $n \in S$, then $2n + 2 \in S$. Give a simple description of the integers in S .

Problem 15.3. Give a recursive definition of the set
 $\{3^n - 3 \mid n \text{ a positive integer}\} = \{0, 6, 24, 78, 240, 726, 2184, \dots\}$.

Problem 15.4. A set S of strings over $\Sigma = \{a, b, c\}$ is defined recursively by (1) $a \in S$, and (2) if $x \in S$ then $bxc \in S$. List all the strings in S of length seven or less.

Problem 15.5. A set S of positive integers is defined recursively by the rules (1) $1 \in S$, and (2) If $n \in S$, then $2n - 1 \in S$. List all the elements in the set S .

Problem 15.6. Give a recursive definition of the set of positive integers that end with the digit 1.

Problem 15.7. Give a recursive definition of the set of strings over the alphabet $\Sigma = \{a, b, c\}$ of the form $aaa \cdots abccc \cdots c$. More carefully: zero or more a 's followed by a single b followed by the same number of c 's as a 's.

Problem 15.8. Describe the strings in the set S of strings over the alphabet $\Sigma = \{a, b, c\}$ defined recursively by (1) $a \in S$ and (2) if $x \in S$ then $ax \in S$ and $xb \in S$ and $xc \in S$.

Hint: Your description should be a sentence that provides an easy test to check if a given string is in the set or not. An example of such a description is: S consists of all strings of a 's, b 's, and c 's, with more a 's than b 's. That isn't a correct description since abb is in S and doesn't have more a 's than b 's, and also $baac$ isn't in S , but does have more a 's than b 's. So that attempted description is really terrible. One way to do this problem is to use the rules to build a bunch of strings in S until a suitable description becomes obvious. Alternatively, just thinking about the recursive rules might be sufficient for you to see a simple description of the strings in S .

Problem 15.9. A set S of ordered pairs of integers is defined recursively by (1) $(1, 1) \in S$, and (2) if $(m, n) \in S$, then $(m + 2, n) \in S$ and $(m, n + 2) \in S$ and $(m + 1, n + 1) \in S$. Give a simple description of the ordered pairs in S .

Chapter 16: Mathematical Induction

As mentioned earlier, to show that a proposition of the form $\forall x P(x)$ is true, it is necessary to check that $P(c)$ is true for every possible choice of c in the domain of discourse. If that domain is not too big, it is feasible to check the truth of each $P(c)$ one by one. For instance, consider the proposition *For every page in these notes, the letter e appears at least once on the page*. To express the proposition in symbolic form we would let the domain of discourse be the set of pages in these notes, and we would let the predicate E be *has an occurrence of the letter e*, so the proposition becomes $\forall p E(p)$. The truth value of this proposition can be determined by the tedious but feasible task of checking every page of the notes for an e. If a single page is found with no e's, that page would constitute a counterexample to the proposition, and the proposition would be false. Otherwise it is true.

When the domain of discourse is a finite set, it is, in principle, always possible to check the truth of a proposition of the form $\forall x P(x)$ by checking the members of the domain of discourse one by one. But that option is no longer available if the domain of discourse is an infinite set since no matter how quickly the checks are made there is no practical way to complete the checks in a finite amount of time.

For example, consider the proposition *For every natural number n , $n^5 - n$ ends with a 0*. Here the domain of discourse is the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. The truth of the proposition could be established by checking:

$0^5 - 0 = 0$	$1^5 - 1 = 0$	$2^5 - 2 = 30$	$3^5 - 3 = 240$
$4^5 - 4 = 1020$	$5^5 - 5 = 3120$	$6^5 - 6 = 7770$	$7^5 - 7 = 16800$
$8^5 - 8 = 32760$	$9^5 - 9 = 59040$	$10^5 - 10 = 99990$	$11^5 - 11 = 161040$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

(and so on forever.)

Checking these facts one by one is obviously a hopeless task, and, of course, just checking a few of them (or even a few billion of them) will never suffice to prove they are all true. And it is not sufficient to check a few and say that the facts are all clear. That's not a proof, it's only a suspicion. So, verifying the truth of $\forall n (n^5 - n) \text{ ends with a } 0$ for domain of discourse $\mathbb{N}$ seems tough.

Proving a universally quantified statement when the domain of discourse is an infinite set can be a tough nut to crack. But, when the domain of discourse is the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, there is a technique called **mathematical induction** that comes to the rescue.

The method of proof by induction provides a way of checking that all the statements in the list are true without actually verifying them one at a time. The process is carried out in two steps. First (the **basis step**) we check that the first statement in the list is correct. Next (the **inductive step**), we show that if any statement in the list is known to be correct, then the one following must also be correct. Putting these two facts together, it ought to appear reasonable that all the

statements in the list are correct. In a way, it's amazing: we learn infinitely many statements are true just by checking two facts. It's like killing infinitely many birds with two stones.

So, suppose a list of statements, $p(0), p(1), p(2), \dots, p(k), p(k + 1) \dots$ is presented and we want to show they are all true. The plan is to show two facts:

- (1) $p(0)$ is true, and
- (2) for any $n \in \mathbb{N}, p(n) \rightarrow p(n + 1)$.

We then conclude all the statements in the list are true.

The **well ordering property** of the positive integers provides the justification for proof by induction. This property asserts that every non-empty subset of the natural numbers contains a smallest number. In fact, given any nonempty set of natural numbers, we can determine the smallest number in the set by the process of checking to see, in turn, if 0 is in the set, and, if the answer is *no*, checking for 1, then for 2, and so on. Since the set is nonempty, eventually the answer will be *yes, that number is in the set*, and in that way, the smallest natural number in the set will have been found. Now let's look at the proof that induction is a valid form of proof. The statement of the theorem is a little more general than described above. Instead of beginning with a statement $p(0)$, we allow the list to begin with a statement $p(k)$ for some integer k (almost always, $k = 0$ or $k = 1$ in practice). This does not have any effect of the concept of induction. In all cases, we have a list of statements, and we show the first statement is true, and then we show that if any statement is true, so is the next one. The particular starting point of the list doesn't really matter. It only matters that there is a starting point.

Theorem 16.1 (Principle of Mathematical Induction). *Suppose we have a list of statements*

$$p(k), p(k + 1), p(k + 2), \dots, p(n), p(n + 1) \dots$$

If (1) $p(k)$ is true, and (2) $p(n) \rightarrow p(n + 1)$ for every $n \geq k$, then all the statements in the list are true.

Proof. The proof will be by contradiction.

Suppose that (1) and (2) are true, but that it is not the case that $p(n)$ is true for all $n \geq k$.

Let $S = \{n | n \geq k \text{ and } p(n) \text{ is false}\}$, so that $S \neq \emptyset$. Since S is a non-empty set of integers greater than or equal to k it has a least element, say t . So, t is the smallest positive integer for which $p(n)$ is false. In the ever-colorful jargon of mathematics, t is usually called the *minimal criminal*.

Since $p(k)$ is true, $k \notin S$. Therefore $t > k$. Whence $t - 1 \geq k$. Since t is the smallest integer greater than or equal to k for which p is false, it must be that $p(t - 1)$ is true. Now by part (2), we also know that $p(t - 1) \rightarrow p(t)$ is true. So it must be that $p(t)$ is true. $\rightarrow \leftarrow$ ■

A handy way of viewing mathematical induction is to compare proving the sequence

$$p(k) \wedge p(k + 1) \wedge p(k + 2) \wedge \dots \wedge p(m) \dots$$

to knocking down a set of dominos set on edge and numbered consecutively $k, k + 1, \dots$. If we want to knock all of the dominos down, which are numbered k and greater, then we must knock the k th domino down, and ensure that the spacing of the dominos is such that every domino will knock down its successor. If either the spacing is off ($\exists m \geq k$ with $p(m)$ not implying $p(m + 1)$), or if we fail to knock down the k th domino (we do not demonstrate that $p(k)$ is true), then there may be dominoes left standing.

Many people find proofs by induction a little bit black-magical at first, just keep the goals in mind: namely check (1) the first statement in the list is true, and (2) that if any statement in the list is true, so is the one that follows it.

When checking the inductive step, $p(n) \rightarrow p(n + 1)$, the statement $p(n)$, is called the **inductive hypothesis**.

To discover how to prove the inductive step most people start by explicitly listing several of the first instances of the inductive hypothesis $p(n)$. Then, look for how to make, in a general way, an argument from one, or more, instances to the next instance of the hypothesis. Once an argument is discovered that allows us to advance from the truth of previous one, or more, instances, that argument, in general form, becomes the pattern for the proof on the inductive hypothesis. Let's examine an example.

Example 16.2. *Let's prove that, for each positive integer n , the sum of the first n positive integers is equal to $n(n + 1)/2$. Here is the list of statements we want to verify.*

$p(1):$	$1 = \frac{1(1 + 1)}{2}$	<i>To get $p(2)$ add 2 to both sides</i>
$p(2):$	$1 + 2 = \frac{2(2 + 1)}{2}$	<i>To get $p(3)$ add 3 to both sides</i>
$p(3):$	$1 + 2 + 3 = \frac{3(3 + 1)}{2}$	<i>You will need to simplify each step</i>
$p(4):$	$1 + 2 + 3 + 4 = \frac{4(4 + 1)}{2}$	$\vdots$
$\vdots$	$\vdots$	
$p(n):$	$1 + 2 + \dots + n = \frac{n(n + 1)}{2}$	
$p(n + 1):$	$1 + \dots + n + (n + 1) = \frac{(n + 1)(n + 2)}{2}$	

Once you figure out the general form of the argument that takes us from one instance of $p(l)$ to the next, you have the form of the inductive argument.

Proof. Basis: Let's check the first statement in the list, $p(1)$: $1 = 1(1 + 1)/2$, is correct.

The left-hand side is 1, and the right-hand side is $1(1 + 1)/2 = 2/2 = 1$, so the two sides are equal as claimed.

Inductive Step: Suppose $p(k)$ is true for some integer $k \geq 1$. To be as precise as possible we should suppose $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$ is true for some integer $k \geq 1$.

*(We need to show $p(k + 1)$ is true: we need to verify $1 + 2 + \cdots + (k + 1) = \frac{(k+1)(k+2)}{2}$. But we don't write this down since it would be **assuming the conclusion**.)*

Here are the computations which provide justification of the inductive step:

$$\begin{aligned} 1 + 2 + \cdots + (k + 1) &= 1 + 2 + \cdots + k + (k + 1) \\ &= \frac{k(k + 1)}{2} + (k + 1) \text{ using the inductive hypothesis} \\ &= \frac{k(k + 1)}{2} + \frac{2(k + 1)}{2} \\ &= \frac{k(k + 1) + 2(k + 1)}{2} = \frac{(k + 1)(k + 2)}{2} \end{aligned}$$

Since we have shown what we set out to, we conclude that $p(n)$ is true for all $n \geq 1$. ■

Notice that in the previous proof we used the following strategy to prove equality: start on one side of the equation, $p(k + 1)$ in this case, and work until we arrive at the other side of the equation. We did this through a series of algebraic manipulations and used the induction hypothesis along the way. This will be our general strategy when writing induction proofs.

The next example re-proves the formula for the sum of finitely many terms of a geometric sequence. We will discuss that standard case where the sequence is the powers of a nonzero real number r starting with $r^0 = 1$: $1, r, r^2, \dots, r^n, \dots$. You may be familiar with the version from calculus where we seek to sum $a + ar + ar^2 + \cdots + ar^n$. Our formula will suffice since we can re-write $a + ar + ar^2 + \cdots + ar^n = a(1 + r + \cdots + r^n)$. Since the case $r = 1$ is trivial we shall assume that $r \neq 1$.

Example 16.3. *Let $1 \neq r$ be a nonzero real number. For $n \geq 0$ we have*

$$1 + r + r^2 + \cdots + r^n = \sum_{k=0}^n r^k = \frac{r^{n+1} - 1}{r - 1}.$$

Proof. Basis: When $n = 0$, $1 + r + r^2 + \cdots + r^n = 1 = \sum_{k=0}^0 r^k$ since we have a single term. On the other hand, $\frac{r^{n+1}-1}{r-1} = \frac{r^{0+1}-1}{r-1} = 1$, since $r \neq 1$.

Inductive Step: Now suppose that $1 + r + r^2 + \cdots + r^m = \frac{r^{m+1}-1}{r-1}$ for some integer $m \geq 0$. Then

$$\sum_{k=0}^{m+1} r^k = (1 + r + r^2 + \cdots + r^m) + r^{m+1} \text{ by recursive definition of a sum.}$$

$$= \frac{r^{m+1} - 1}{r - 1} + r^{m+1} \text{ by induction hypothesis.}$$

$$= \frac{r^{m+1} - 1}{r - 1} + \frac{r^{m+2} - r^{m+1}}{r - 1}$$

$$= \frac{r^{m+1} - 1 + r^{m+2} - r^{m+1}}{r - 1}$$

$$= \frac{r^{m+2} - 1}{r - 1}. \blacksquare$$

Example 16.4. For every integer $n \geq 2$, $2^n > n + 1$.

Proof. Basis: When $n = 2$ the inequality to check is $2^2 > 2 + 1$ which is true.

Inductive Step: Now suppose that $2^k > k + 1$ for some integer $k \geq 2$. Then

$$2^{k+1} = 2 \cdot 2^k > 2(n + 1) = 2n + 2 > n + 2. \blacksquare$$

Example 16.5. Of historical interest is the fact that one can show that using only 5¢ stamps and 9¢ stamps, any postage amount 32¢ or greater can be formed.

To re-phrase: Any integer $n \geq 32$ is a linear combination of 5 and 9 with natural number coefficients. Once more: If $n \geq 32$, then $n = 5k + 9l$ for some $k, l \in \mathbb{N}$.

Proof. Basis: $32 = 1 \cdot 5 + 3 \cdot 9$ so the base case is true.

Inductive Step: Now suppose that we can write $n = 5k + 9l$ for some integer $n \geq 32$, where $k, l \in \mathbb{N}$. We need to show that we can write $n + 1 = 5m + 9j$ for some natural numbers j, m . Since $n \geq 32$ we must either have 1) $k \geq 7$ or 2) $l \geq 1$. Otherwise $k < 7$ and $l = 0$ so that we have $n \leq 6 \cdot 5 = 30 \rightarrow \leftarrow$.

Case 1: If $k \geq 7$ we can write $n + 1 = (k - 7) \cdot 5 + (l + 4) \cdot 9$.

Case 2: If $l \geq 1$ we can write $n + 1 = (k + 1) \cdot 5 + (l - 1) \cdot 9. \blacksquare$

Example 16.4. Now let us look at an example of an induction proof with a geometric flavor. Suppose that we have a 4×5 chessboard and a supply of 1×2 dominoes.

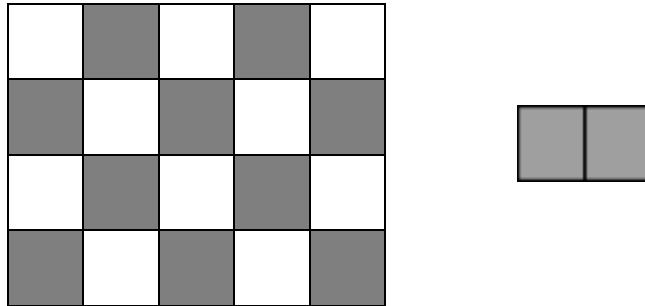


Figure 16.1: 4×5 chessboard and 1×2 domino

Each domino covers exactly two squares on the board. A **perfect cover** of the board consists of a placement of dominoes on the board so that each domino covers two squares on the board (dominoes can be either vertically or horizontally oriented), no dominoes overlap, no dominoes extend beyond the edge of the board, and all squares on the board are covered by a domino. It's easy to see that the 4×5 board above has a perfect cover. In general, you should be able to prove:

Theorem 16.7. *An $m \times n$ board has a perfect cover if and only if at least one of m and n is even.*

There is a second form of mathematical induction. Anything that can be proven with this second version can be proven with the method described above, and vice versa, but this second version is often easier to use. The change occurs in the induction hypothesis. Instead of assuming $p(m)$ is true for some $m \geq k$ and proving $p(m + 1)$ we assume $p(j)$ is true for $k \leq j \leq m$ and then prove $p(m + 1)$. This is described in the following theorem:

Theorem 16.8. (Second Principle of Mathematical Induction) *For integers n and k if*

- 1) $p(k)$ is true, and
 - 2) $[p(k) \wedge p(k + 1) \wedge \dots \wedge p(m)] \rightarrow p(m + 1)$ for an arbitrary $m \geq k$
- then $p(n)$ is true for all $n \geq k$.*

This principle is shown to be valid in the same manner as the first form of induction was justified. The utility lies in dealing with cases where we want to use inductive reasoning, but cannot deduce the $(n + 1)$ st case from the n th case directly. Let's do a few examples of proofs using this second form of induction. But first, we comment that in many induction proofs, it is convenient to check several initial cases in the basis step to avoid having to use proof by cases in the inductive step.

Example 16.9. *For any integer $n \geq 32$ we can write $n = 5k + 9l$ for some $k, l \in \mathbb{N}$.*

Proof. We can write

$$32 = 1 \cdot 5 + 3 \cdot 9$$

$$33 = 3 \cdot 5 + 2 \cdot 9$$

$$34 = 5 \cdot 5 + 1 \cdot 9$$

$$35 = 7 \cdot 5 + 0 \cdot 9$$

$$36 = 0 \cdot 5 + 4 \cdot 9$$

Inductive Step: Suppose that for some integer m with $m \geq 36$ we can write $j = 5 \cdot k_j + 9 \cdot l_j$ for natural numbers k_j, l_j and for $32 \leq j \leq m$. Then since $32 \leq m - 4$, by inductive hypothesis we can write $m - 4 = 5 \cdot k_{m-4} + 9 \cdot l_{m-4}$ for some natural numbers k_{m-4}, l_{m-4} . Therefore we can write $m + 1 = 5 \cdot (k_{m-4} + 1) + 9 \cdot l_{m-4}$ where $k_{m-4} + 1, l_{m-4} \in \mathbb{N}$. ■

Example 16.10. *Induction can be used to verify a guessed, closed form for a recursively defined sequence. Consider the sequence defined recursively by the initial conditions $a_0 = 2, a_1 = 5$ and the recursive rule for $n \geq 2, a_n = 5a_{n-1} - 6a_{n-2}$. The first few terms of this sequence are 2, 5, 13, 35, 97, A little experimentation leads to the guess $a_n = 2^n + 3^n, n \geq 0$. Let's verify that guess using induction. For the basis of the induction we check $2 = a_0 = 2^0 + 3^0$ and also $5 = a_1 = 2^1 + 3^1$. So far, so good. For the inductive step let's suppose that our guess is correct for all k with $2 \leq k \leq m$ for some integer m . That is $a_k = 2^k + 3^k$ for $2 \leq k \leq m$. Then'*

$$\begin{aligned} a_{m+1} &= 5a_m - 6a_{m-1} \\ &= 5(2^m + 3^m) - 6(2^{m-1} + 3^{m-1}), \text{ by inductive hypothesis} \\ &= (5 \cdot 2 - 6)2^{m-1} - (6 - 5 \cdot 3)3^{m-1}, \text{ collecting like terms} \\ &= 4 \cdot 2^{m-1} - (-9) \cdot 3^{m-1} = 2^2 2^{m-1} + 3^2 3^{m-1} \\ &= 2^{m+1} + 3^{m+1}. \blacksquare \end{aligned}$$

Example 16.11. *In the game of Nim, two players are presented with a pile of matches. The players take turns removing one, two or three matches at a time. The player forced to take the last match is the loser. For example, if the pile initially contains 8 matches, then the first player can, with correct play, be sure to win. Here's how: Player 1 takes 3 matches leaving 5; player 2's options will leave 4, 3 or 2 matches; so player 1 then takes 3, 2 or 1 matches accordingly, leaving player 2 with the last match. Notice that if player one incorrectly plays by taking only 1 or 2 matches on her first turn she is bound to lose to good play since player 2 can then reduce the pile to 5 matches guaranteeing her the win.*

Let's prove that if the number of matches in the pile is 1 more than a multiple of 4, the second player can force a win; otherwise the first player can force a win.

Proof. For the basis we note that obviously the second player wins if there is only one match in the pile. Also for 2, 3 or 4 matches player one reduces the pile to one match and is guaranteed the win.

For the inductive step suppose for all $1 \leq k \leq m$ and some $m \geq 4$; if there are k matches in the pile and k is 1 more than a multiple of 4, the second player can force a win; otherwise the first player can force a win.

Case 1: If $k + 1$ is 1 more than a multiple of 4, then when player one takes her matches, the pile will not contain 1 more than a multiple of 4 matches. Thus player 2 can force a win by the induction hypothesis.

Case 2: If $k + 1$ is not 1 more than a multiple of 4, then player one can select matches so that there are 1 more than a multiple of 4 at the end of her turn. She thus guarantees herself the win by induction hypothesis. $\blacksquare$

So, to win at Nim leave one more match than a multiple of four when it is your turn if possible. Of course if your opponent knows the rules for good play, you might just as well count the number of matches to determine who will win since there is not a good reason to play.

Exercises

Exercise 16.1. Use induction to prove that for every integer $n \geq 1$, is

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}.$$

Exercise 16.2. Prove that for every integer $n \geq 1$,

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1) 2^{n+1} + 2.$$

Exercise 16.3. The Fibonacci sequence is defined recursively by $f_0 = 0$, $f_1 = 1$, and, for $n \geq 2$,

$f_n = f_{n-1} + f_{n-2}$. Use induction to prove that for all $n \geq 0$, $f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$.

Exercise 16.4. Prove by induction: For every integer $n > 4$, we have $2^n > n^2$.

Exercise 16.5. Prove by induction: For every integer $n \geq 0$, $11^n - 6$ is divisible by 5.

Exercise 16.3. A pizza is cut into pieces (maybe some pretty oddly shaped) by making some integer $n \geq 0$ number of straight-line cuts. Prove: The maximum number of pieces is $(n^2 + n + 2)/2$.

Exercise 16.7. A sequence is defined recursively by $a_0 = 0$, and, for $n \geq 1$, $a_n = 5a_{n-1} + 1$. Use induction to prove the closed form formula for a_n is

$$a_n = \frac{5^n - 1}{4}.$$

Exercise 16.8. A sequence is defined recursively by $a_0 = 1$, $a_1 = 4$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$. Use induction to prove that the closed form formula for a_n is $a_n = 2 \cdot 3^n - 2^n$, $n \geq 0$.

Problems

Problem 16.1. Prove for every integer $n \geq 1$,

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Problem 16.2. Prove by induction: For $n \geq 2$,

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

Problem 16.3. Show that any integer $n \geq 8$ can be written as a linear combination of the integers 3 and 5 using nonnegative integers as coefficients. That is if $n \geq 8$, there exist nonnegative integers k_n, l_n so that $n = 3 \cdot k_n + 5 \cdot l_n$. Do this twice, using both styles of induction.

Problem 16.4. Prove by induction: For every integer $n \geq 1$,

$$\sum_{k=1}^n (-1)^k k^2 = (-1)^n \frac{n(n+1)}{2}.$$

Problem 16.5. Prove by induction: For every integer $n \geq 1$, the number $n^5 - n$ is divisible by 5.

Problem 16.6. Prove by induction: For the Fibonacci sequence and for all $n \geq 2$,

$$f_0^2 + f_1^2 + f_3^2 + \cdots + f_n^2 = f_n f_{n+1}.$$

Problem 16.7. Prove by induction: For the Fibonacci sequence and for all $n \geq 2$,

$$f_{n-1} f_{n+1} = f_n^2 + (-1)^n.$$

Problem 16.8. Here is a proof that for $n \geq 0$, $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1}$.

Proof. Suppose $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1}$ for some $n \geq 0$. Then

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^n + 2^{n+1} &= 2^{n+1} + 2^{n+1} \quad \text{using the inductive hypothesis} \\ &= 2 \cdot 2^{n+1} = 2^{n+2} = 2^{(n+1)+1}. \blacksquare \end{aligned}$$

Now, obviously there is something wrong with this proof since for example $1 + 2 + 2^2 = 7$, but we have $2^{2+1} = 2^3 = 8$. Where does the proof go bad?

Chapter 17: Algorithms

An **algorithm** is a recipe to solve a problem. For example, here is an algorithm that solves the problem of finding the distance traveled by a car given the time it has traveled t and its average speed s : multiply t and s .

Over time, the requirements of what exactly constitutes an algorithm have matured. A really precise definition would be filled with all sorts of technical jargon, but the ideas are commonsensible enough that an informal description will suffice for our purposes. So, suppose we have in mind a certain class of problems (such as determine the distance traveled given time traveled and average speed). The properties of an algorithm to solve examples of that class of problems are:

- (1) **Input:** The algorithm is provided with data.
- (2) **Output:** The algorithm produces a solution.
- (3) **Definiteness:** The instructions that make up the algorithm are precisely described. They are not open to interpretation.
- (4) **Finiteness:** The output is produced in a finite number of steps.
- (5) **Generality:** The algorithm produces correct output for any set of input values.

The algorithm for finding distance traveled given time traveled and average speed obviously meets all five requirements of an algorithm. Notice that, in this example, we have assumed the user of the algorithm understands what it means to multiply two numbers. If we cannot make that assumption, then we would need to add a number of additional steps to the algorithm to solve the problem of multiplying two numbers together. Of course, that would make the algorithm significantly longer. When describing algorithms, we'll assume the user knows the usual algorithms for solving common problems such as addition, subtraction, multiplication, and division of numbers, and knows how to determine if one number is larger than another etc.

Just as important as an example of what an algorithm is, is an example of what is not an algorithm. For example, we might describe the method by which most people used to look up a number in a phone book. One would open the book and look to see if the listing you're looking for is on that page or not. If it is you find the number using the fact that the listings are alphabetized and you're done. If the number you're looking for is not on the page, you use the fact that the listings are alphabetized to either flip back several pages, or forward several pages. This page is checked to see if the listing is on it. If it is not we repeat the process. One problem in this case is that this description is not definite. The phrase *flip back several pages* is too vague, it violates the definiteness requirement. Another problem is that someone could flip back and forth between two pages and never find the number, and so violate the finiteness requirement. So this method is not an algorithm.

Continuing the example from above of looking up an item indexed by a sorted list, one algorithm for completing this is to look at the first entry in the list. If it's the item you're looking for you're done. Else move to the next entry. It's either the item you're looking for or you move to the next

entry. This is an example of a **linear search algorithm**. It's not too bad for finding an early entry in the list, but awful for later entries in the list.

Another algorithm to complete that task of looking up an item indexed by a sorted list is the **binary search algorithm**. We first consider the middle entry. If it's the item we're looking for, we're done. Else we know the item is in the first half of the list, or the last half of the list since the entries are ordered. We then pick the middle entry of the appropriate half, and repeat the halving process on that half, until eventually the item is located. There are a few details to fix up to make this a genuine algorithm. For example, what is the middle entry if there are an even number of items listed? Also, what happens if the item we are looking for isn't in the list? But it is clear with a little effort we can add a few lines to the instructions to make this process into an algorithm.

It is traditional to present algorithms in a *pseudocode* form like a program for a computer. For instance, the linear search algorithm can be written in pseudocode form as shown in Algorithm 1.

Algorithm 1 Linear search (for loop)

Input: $(name, phonelist)$

Output: $phonelist(namespot)$ = phone number of name in phonelist

1: **for** $namespot$ in $\{1, 2, \dots, \text{length}(phonelist)\}$ **do**

2: **if** $listnamespot = name$ **then**

3: **output** $phonelist(namespot)$

4: **stop**

5: **end if**

6: **end for**

7: **output** $name$ not found

8: **stop**

Example 17.1. Here is an algorithm for determining $\lfloor m/n \rfloor$ for positive integers m, n .

Algorithm 2 Calculate $\lfloor m/n \rfloor$

Input: positive integers m and n

Output: integer value of m/n

1: $k \leftarrow 0$ $\triangleright k$ will eventually hold our answer

2: **while** $m \geq 0$ **do**

3: $m \leftarrow m - n$ $\triangleright$ We're doing division by repeated subtraction

4: $k \leftarrow k + 1$

▷ k counts the number of subtractions

5: **end while**

6. **output** $k - 1$

▷ We counted one too many subtraction (How?)

*Here are the sequence of steps this algorithm would carry out with input $m = 23$ and $n = 7$:
[initial status. $m = 23, n = 7, k = (\text{undefined})$]*

instr 1: Set k to be 0 [status: $m = 23, n = 7, k = 0$]

instr 2: is $m \geq 0$? Yes, $(23 \geq 0)$ is true. Do next instruction (i.e. instr 3).

instr 3: m reset to be $m - n = 23 - 7 = 16$. [status: $m = 16, n = 7, k = 0$]

instr 4: k reset to be $k + 1 = 0 + 1 = 1$. [status: $m = 16, n = 7, k = 1$]

*instr 5: jump back to the matching **while** (i.e. instr 2).*

instr 2: is $m \geq 0$? Yes, $(16 \geq 0)$ is true. Do next instruction.

instr 3: m reset to be $m - n = 16 - 7 = 9$. [status: $m = 9, n = 7, k = 1$]

instr 4: k reset to be $k + 1 = 1 + 1 = 2$. [status: $m = 9, n = 7, k = 2$]

*instr 5: jump back to the matching **while**.*

instr 2: is $m \geq 0$? Yes, $(9 \geq 0)$ is true. Do next instruction.

instr 3: m reset to be $m - n = 9 - 7 = 2$. [status: $m = 2, n = 7, k = 2$]

instr 4: k reset to be $k + 1 = 2 + 1 = 3$. [status: $m = 2, n = 7, k = 3$]

*instr 5: jump back to the matching **while**.*

instr 2: is $m \geq 0$? Yes, $(2 \geq 0)$ is true. Do next instruction.

instr 3: m reset to be $m - n = 2 - 7 = -5$. [status: $m = -5, n = 7, k = 3$]

instr 4: k reset to be $k + 1 = 3 + 1 = 4$. [status: $m = -5, n = 7, k = 4$]

*instr 5: jump back to the matching **while**.*

*instr 2: is $m \geq 0$? **No**, $(-5 \geq 0)$ is false. Jump to instr after **end while**.*

*instr 6: **output** value of $k - 1$ (i.e. 3). [status: $m = -5, n = 7, k = 4$]*

stop! (This is what happens when there are no more instructions to execute.)

Here is a second algorithm for the same problem.

Algorithm 3 Calculate $\lfloor m/n \rfloor$ (again)

Input: positive integers m and n

Output: integer value of $\lfloor m/n \rfloor$

divide m by n to one place beyond the decimal, call the result r .

output the digits of r preceding the decimal point.

So, given the input $m = 23$ and $n = 7$ we go through the steps.

instr 1: $r = 3.2$

instr 3: Output 3.

stop!

Problems

Problem 17.1. Consider the following algorithm: The input will be 2 integers $m \geq 0$ and $n \geq 1$.

Input: integers $m \geq 0, n \geq 1$

Output: (to be determined)

$s \leftarrow 0$

while $m \neq 0$ **do**

$s \leftarrow n + s$

$m \leftarrow m - 1$

end while

output s

Describe in words what this algorithm does. In other words, what problem does this algorithm solve?

Problem 17.2. Consider the following algorithm: The input will be any integer $n > 1$.

Input: integer $n > 1$

Output: (to be determined)

$t \leftarrow 0$

while n is even **do**

$t \leftarrow t + 1$

$n \leftarrow n/2$

end while

output t

- a) List the steps the algorithm follows for the input $n = 12$.
- b) Describe in words what this algorithm does. In other words, what problem does this algorithm solve?

Problem 17.3. Design an algorithm that takes any positive integer n and returns half of n if it is even and half of $n + 1$ if it is odd. (Such an algorithm is often needed in computer science.)

Problem 17.4. Consider the following algorithm: The input will be a function f together with its finite domain $D = \{d_1, d_2, \dots, d_n\}$.

Input: function f with domain $D = \{d_1, d_2, \dots, d_n\}$

Output: (to be determined)

```

1:  $i \leftarrow 1$ 
2: while  $i < n$  do
3:    $j \leftarrow i + 1$ 
4:   while  $j < n$  do
5:     if  $f(d_i) = f(d_j)$  then
6:       output NO
7:       stop
8:     end if
9:      $j \leftarrow j + 1$ 
10:  end while
11:   $i \leftarrow i + 1$ 
12: end while
13: output YES

```

- a) List the steps the algorithm follows for the input $f: \{a, b, c, d, e\} \rightarrow \{\alpha, \beta, \gamma, \delta, \zeta, \eta\}$ given by $f(a) = \alpha, f(b) = \delta, f(c) = \eta, f(d) = \alpha, f(e) = \gamma$.
- b) Describe in words what this algorithm does. In other words, what problem does this algorithm solve?

Problem 17.5. Design an algorithm that will convert the ordered triple (a, b, c) to the triple (b, c, a) . For example, if the input is $(7, X, *)$, the output will be $(X, *, 7)$.

Problem 17.6. Design an algorithm whose input is a finite list of positive integers and whose output is the sum of the even integers in the list. If there are no even integers in the list, the output should be 0.

Problem 17.7. A *palindrome* is a string of letters that reads the same in each direction. For example, *refer* and *redder* are palindromes of length five and six respectively. Design an algorithm that will take a string as input and output yes if the string is a palindrome, and no if it is not.

Chapter 18: Algorithm Efficiency

There are many different algorithms for solving any particular class of problems. In the last chapter, we considered two algorithms for solving the problem of looking up a phone number, given a person's name.

Algorithm L: Look at the first entry in the book. If it's the number you're looking for you're done. Else move to the next entry. It's either the number you're looking for, or you move to the next entry, and so on. (The **linear search algorithm**)

Algorithm B: The second algorithm took advantage of the arrangement of a phone book in alphabetical order. We open the phone book to the middle entry. If it's the number we're looking for, we're done. Otherwise, we know the number is listed in the first half of the book, or the last half of the book. We then pick the middle entry of the appropriate half and repeat the process. After some number of repetitions, we will either be at the name we want, or learn the name isn't in the book. (The **binary search algorithm**)

The question arises, which algorithm is *better*? The question is vague. Let's assume that *better* means *uses fewer steps*. Now if there are only one or two names in the phone book, it doesn't matter which algorithm we use, the look-up always takes one or two steps. But what if the phone book contains 10000 names? In this case, it is hard to say which algorithm is better: looking up Adam Aaronson will likely only take one step by the linear search algorithm, but binary search will take 14 steps or so. But for Zebulon Zyzniewski, the linear search will take 10000 steps, while the binary search will again take about 14 steps.

There are two lessons to be learned from those last examples:

- (1) Small cases of the problem can be misleading when judging the quality of an algorithm.
- (2) It's unlikely that one algorithm will always be more efficient than another.

The common approach to compare the efficiency of two algorithms takes those two lessons into account by agreeing to the following protocol:

- (1) Only compare the algorithms when the size n of the problem it is applied to is huge. In the phone book example, don't worry about phone books of 100 names or even 10000 names. Worry instead about phone books with n names where n gets arbitrarily large.
- (2) To compare two algorithms, first, for each algorithm, find the maximum number of steps ever needed when applied to a problem of size n . For a phone book of size n the linear search algorithm will require n steps in the worst possible case of the name not being in the book. On the other hand, the halving process of the binary search algorithm means that it will never take more than about $\log_2 n$ steps to locate a name (or discover the name is missing) in the phone book. This information is expressed compactly by saying the linear search algorithm has **worst case scenario** efficiency $\omega_L(n) = n$ while the binary search algorithm has worst case scenario efficiency $\omega_B(n) = \log_2 n$.

- (3) We declare that algorithm #1 is **more efficient** than algorithm #2 provided, for all problems of huge sizes n , $\omega_1(n) < \omega_2(n)$, where ω_1 and ω_2 are the worst-case scenario efficiencies for each algorithm.

Notice that for huge n , $\omega_B(n) < \omega_L(n)$. In fact, there is no real contest. When $n = 1048576 = 2^{20}$, we get $\omega_B(n) = 20$ while $\omega_L(n) = 1048576$, and things only get better for $\omega_B(n)$ as n gets larger.

In summary, to compare two algorithms designed to solve the same class of problems we:

- (1) Determine a number n that indicates the size of the problem. For example, if the algorithm manipulates a list of numbers, n could be the length of the list. If the algorithm is designed to raise a number to a power, the size could be the power n .
- (2) Decide what will be called a *step* when applying the algorithms. In the phone book example, we took a step to mean a comparison. When raising a number to a power, a step might consist of performing a multiplication. A step is usually taken to be the most time-consuming action in the algorithm, and other actions are ignored. Also, when determining the function, we don't get hung up worrying about minuscule details. Don't spend time trying to determine if $\omega(n) = 2n + 7$ or $\omega(n) = 2n + 67$. For huge values of n , the $+7$ and $+67$ become unimportant. In such a case, $\omega(n) = 2n$ has all the interesting information. Don't sweat the small stuff.
- (3) Determine the worst-case scenario functions for the two algorithms and compare them. The smaller of the two (assuming they are not essentially the same) is declared the more efficient algorithm.

Example 18.1. *Let's do a worst-case scenario computation for the following algorithm designed to determine the largest number in a list of n numbers. It would be natural to use the number of items in the list, n , to represent the size of a problem. And let's use the comparisons as steps. We are going to make two comparisons for each of the items in the list in every case (every case is a worst case for this algorithm!). So, we give this algorithm an efficiency $\omega(n) = 2n$. Notice that we only need comparisons for the last $n - 1$ items in the list, and the exact number of times the comparisons in instructions (3) and (4) are carried out might take a few minutes to figure out. But it's clear that both are carried out about n times, and since we are only interested in huge n 's, being off by a few (or a few billion) isn't really going to matter at all.*

Algorithm 4: Maximum list value

Input: A list of n numbers $a_1, a_2, \dots, a_n$

Output: $\max(a_1, \dots, a_n)$

1: $\text{max} \leftarrow a_1$

2: $k \leftarrow 2$

3: **while** $k \leq n$ **do**

4: **if** $\text{max} < a_k$ **then**

5: $\text{max} \leftarrow a_k$

6: **end if**

7: $k \leftarrow k + 1$

8: **end while**

9: **output** max

Problems

Problem 18.1. *For the algorithm presented in problem 17.2 from the last chapter:*

- a) *Select a value to represent the size of an instance of the problem the algorithm is designed to solve.*
- b) *Decide what will constitute a step in the algorithm.*
- c) *Determine the worst-case scenario function $\omega(n)$.*

Problem 18.2. *Repeat problem 18.1 for the following algorithm:*

Input: n –tuples of real numbers $(x_1, x_2, \dots, x_n)$ and $(y_1, y_2, \dots, y_n)$

Output: (to be determined)

1: $S \leftarrow 0$

2: $i \leftarrow 1$

3: **while** $i \leq n$ **do**

4: $S \leftarrow S + x_i \cdot y_i$

5: $i \leftarrow i + 1$

6: **end while**

7: **output** S

Chapter 19: The Growth of Functions

Now that we have an idea of how to determine the efficiency of an algorithm by computing its worst-case scenario function, $\omega(n)$, we need to be able to decide when one algorithm is better than another. For example, suppose we have two algorithms to solve a certain problem, the first with $\omega_1(n) = 10000n^2$, and the second with $\omega_2(n) = 2^n$. Which algorithm would be the better choice to implement based on these functions? To find out, let's assume that our computer can carry out one billion steps per second, and estimate how long each algorithm will take to solve a worst-case problem for various values of n .

$\omega(n)$	$n = 10$	$n = 20$	$n = 50$	$n = 100$
$10000n^2$	.001 sec	.004 sec	.025 sec	.1 sec
2^n	.000001 sec	.001 sec	4.2 months	4×10^{11} centuries

Table 19.1: Problem size vs. CPU time used

So, it looks like the selection of the algorithm depends on the size of the problems we expect to run into. Up to size 20 or so, it doesn't look like the choice makes a lot of difference, but for larger values of n , the $10000n^2$ algorithm is the only practical choice.

It is worth noting that the values of the efficiency functions for small values of n can be deceiving. It is also worth noting that, from a practical point of view, simply designing an algorithm to solve a problem without analyzing its efficiency can be a pointless exercise.

There are a few types of efficiency functions that crop up often in the analysis of algorithms. In order of decreasing efficiency for large n they are $\log_2 n$, $\sqrt{n}$, n , n^2 , n^3 , 2^n , $n!$.

Assuming one billion steps per second, here is how these efficiency functions compare for various choices of n .

$\omega(n)$	$n = 10$	$n = 20$	$n = 50$	$n = 100$
$\log_2 n$	.000000003 sec	.000000004 sec	.000000005 sec	.000000006 sec
$\sqrt{n}$	.000000003 sec	.000000004 sec	.000000006 sec	.000000008 sec
n	.00000001 sec	.00000002 sec	.00000004 sec	.00000006 sec
n^2	.0000001 sec	.0000004 sec	.0000016 sec	.0000036 sec
n^3	.000001 sec	.000008 sec	.000064 sec	.00022 sec
2^n	.000001 sec	.001 sec	18.3 minutes	36.5 years
$n!$	.0036 sec	77 years	2.6×10^{29} centuries	2.6×10^{29} centuries

Table 19.2: Common efficiency functions for small values of n

Even though the values in the first five rows of the table look reasonably close together, that is a false impression fostered by the small values of n . For example, when $n = 1000000$, those five entries would be as in table [19.3](#).

$\omega(n)$	$n = 1000000$
$\log_2 n$	.00000002 sec
$\sqrt{n}$	.000001 sec
n	.001 sec
n^2	17 minutes
n^3	31.7 years

Table 19.3: Efficiency functions where $n = 1000000$

And, for even larger values of n , the $\sqrt{n}$ algorithm will require billions more years than the $\log_2 n$ algorithm.

There is a traditional method of estimating the efficiency of an algorithm. As in the examples above, one part of the plan is to ignore tiny contributions to the efficiency function. In other words, we won't write expressions such as $\omega(n) = n^2 + 3$, since the term 3 is insignificant for the large values of n we are interested in. As far as behavior for large values of n is concerned, the functions n^2 and $n^2 + 3$ are indistinguishable. A second part of the plan is to not distinguish between functions if one is always say 10 times the other. In other words, as far as analyzing efficiency, the functions n^2 and $10n^2$ are indistinguishable. And there is nothing special about 10 in those remarks. These ideas lead us to the idea of the order of growth with respect to n , $\mathcal{O}(g(n))$, in the next definition.

Definition 19.1. The function $\omega(n)$ is $\mathcal{O}(g(n))$ provided there is a number $k > 0$ such that $\omega(n) \leq k \cdot g(n)$ for all n (or at least for all large values of n). The symbol $\mathcal{O}(g(n))$ is read in English as *big-oh of $g(n)$* .

As an example, $n^3 + 2n^2 + 10n + 4 \leq (1 + 2 + 10 + 4)n^3 = 17n^3$ is $\mathcal{O}(n^3)$. So if we have an algorithm with efficiency function $\omega(n) = n^3 + 2n^2 + 10n + 4$, we can suppress all the unimportant details, and simply say the efficiency is $\mathcal{O}(n^3)$. In this example, it is also true that $\omega(n)$ is $\mathcal{O}(n^4)$, but that is less precise information. On the other hand, saying $\omega(n)$ is $\mathcal{O}(n^2)$ is certainly false. To indicate that we have the best big-oh estimate allowed by our analysis, we would say $\omega(n)$ is *at best* $\mathcal{O}(n^3)$.

$\mathcal{O}(g(n))$ actually represents the set of functions dominated by $g(n)$. So, it would be proper to write $\omega(n) = n^3 + 2n^2 + 10n + 4 \in \mathcal{O}(n^3)$. Moreover, we could write $\mathcal{O}(n^2) \subset \mathcal{O}(n^3)$ since the functions dominated by n^2 are among those dominated by n^3 . Loosely speaking, finding the $\mathcal{O}$ estimate for a function selects the most influential, or dominant, term (for large values of the variable) in the function, and suppresses any constant factor for that term.

In each of the following examples, we find a big-oh estimate for the given expression.

Example 19.2. We have that $n^4 - 3n^3 + 2n^2 - 6n + 14$ is $\mathcal{O}(n^4)$, since for large n the first term dominates the others.

Example 19.3. For large n , we have the inequalities:

$$(n^3 \log_2 n + n^2 - 3)(n^2 + 2n + 8) \leq (1 + 1 + 3)n^3(\log_2 n)(1 + 2 + 8)n^2 \leq 55n^5 \log_2 n.$$

Hence, $(n^3 \log_2 n + n^2 - 3)(n^2 + 2n + 8)$ is $\mathcal{O}(n^5 \log_2 n)$. Alternatively, we have that $n^3 \log_2 n$ and n^2 dominate their respective factors. Thus, again, the product is $\mathcal{O}(n^5 \log_2 n)$.

The lesson learned is that dominant factors may be multiplied.

Example 19.4. We see that $n^5 + 3(2^n) - 14n^{22} + 13 \leq (1 + 3 + 14 + 13)2^n = 31(2^n)$. Hence, the expression is $\mathcal{O}(2^n)$. Or, since $3 \cdot 2^n$ dominates all the other terms for large n , we see that the expression is $\mathcal{O}(3 \cdot 2^n)$. That is, it's $\mathcal{O}(2^n)$ since the constant factor is irrelevant.

Problems

Problem 19.1. You have been hired for a certain job that can be completed in less than two months and offered two modes of payment. Method 1: You get \$1,000,000,000 a day for as long as the job takes. Method 2: You get \$1 the first day, \$2 the second day, \$4 the third day, \$8 the fourth day, and so on, your payment doubling each day, for as long as the job lasts. Which method of payment do you choose?

Problem 19.2. Suppose an algorithm has efficiency function $\omega(n) = n \log_2 n$. Compute the worst-case time required for the algorithm to solve problems of sizes $n = 10, 20, 40, 60$ assuming the operations are carried out at the rate of one billion per second. Where does this function fit in the table on the second page of this chapter?

Problem 19.3. Repeat problem [19.2](#) for $\omega(n) = n^n$.

Problem 19.4. Explain why $3n^3 + 400n^2 + 2\sqrt{n}$ is at least $\mathcal{O}(n^2)$.

Problem 19.5. Explain why $10n^2 + 4n + 2\sqrt{n}$ is not $\mathcal{O}(1000n)$.

Problem 19.6. Find the best possible big-oh estimate for $\sqrt{5n} + \log_2 10n + 1$.

Problem 19.7. Find the best possible big-oh estimate for $2n^2 + \frac{3}{n}$.

Problem 19.8. Find the best possible big-oh estimate for $\frac{2n^2+2n+1}{2n+1}$. Hint: Use the idea of dominant terms first.

PART IV: Elementary Number Theory

Chapter 20: The Integers

Number theory is concerned with the integers and their properties. In this chapter the rules of the arithmetic of integers are reviewed. The surprising fact is that all the dozens of rules and tricks you know for working with integers (and for doing algebra, which is just arithmetic with symbols) are consequences of just a few basic facts.

The set of **integers**, $\{\dots, -2, -1, 0, 1, 2, \dots\}$, is denoted by the symbol $\mathbb{Z}$. The two familiar arithmetic operations for the integers, addition and multiplication, obey several basic rules. First, notice that addition and multiplication are **binary operations**. In other words, these two operations combine a pair of integers to produce a value. It is not possible to add (or multiply) three numbers at a time. We can figure out the sum of three numbers, but it takes two steps: we select two of the numbers, and add them up, and then add the third to the preliminary total. Never are more than two numbers added together at any time. A list of the seven fundamental facts about addition and multiplication of integers follows.

- 1) The integers are **closed** with respect to addition and multiplication. That means when two integers are added or multiplied, the result is another integer. In symbols

$$\forall a, b \in \mathbb{Z}, ab \in \mathbb{Z} \text{ and } a + b \in \mathbb{Z}.$$

- 2) Addition and multiplication of integers are **commutative** operations. That means that the *order* in which two numbers are combined has no effect on the final answer. In symbols

$$\forall a, b \in \mathbb{Z}, ab = ba \text{ and } a + b = b + a.$$

- 3) Addition and multiplication of integers are **associative** operations. In other words when we compute the sum (or product) of three integers it does not matter whether we combine the first two and then add the third or combine the second two and then add the first. The answer is the same in either case. Symbolically

$$\forall a, b, c \in \mathbb{Z}, (ab)c = a(bc) \text{ and } (a + b) + c = a + (b + c).$$

- 4) There is an **additive identity** denoted by 0. It has the property that when it is added to any integer the result is that integer back again. In symbols

$$\forall a \in \mathbb{Z}, a + 0 = a = 0 + a.$$

- 5) Every integer has an **additive inverse**. $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}$ so that $a + b = 0 = b + a$. As usual, b is denoted by $-a$, so we write $a + (-a) = 0 = (-a) + a$.

- 6) The integer 1 is a **multiplicative identity**. That is, $\forall a \in \mathbb{Z}, a \cdot 1 = a = 1 \cdot a$.

- 7) Multiplication distributes over addition. In symbols $\forall a, b, c \in \mathbb{Z}, a(b + c) = ab + ac$.

The preceding facts tell all there is to know about arithmetic. Every other fact can be proven from these. For example, here is a proof of the cancellation law for addition using the axioms 1) through 7).

Theorem 20.1. (Cancellation Law) *For integers a, b, c , if $a + c = b + c$, then $a = b$.*

Proof. Suppose that $a + c = b + c$. Add $-c$ to both sides of the equation (applying axiom 5) to get $(a + c) + (-c) = (b + c) + (-c)$. By axiom 3 $a + (c + (-c)) = b + (c + (-c))$. By axiom 5 we have $a + 0 = b + 0$. And by axiom 4 we arrive at $a = b$. ■

Theorem 20.2. *For any integer a , $a \cdot 0 = 0$.*

Proof. Here are the steps in the proof. You supply the justifications for the steps.

$$\begin{aligned} a \cdot 0 &= a(0 + 0) \\ a \cdot 0 &= a \cdot 0 + a \cdot 0 \\ a \cdot 0 + (-(a \cdot 0)) &= (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) \\ a \cdot 0 + (-(a \cdot 0)) &= a \cdot 0 + (a \cdot 0 + (-(a \cdot 0))) \\ 0 &= a \cdot 0 + 0 \\ 0 &= a \cdot 0. \quad \blacksquare \end{aligned}$$

Your justification for each step should be stated as using one, or more, of the fundamental facts as applied to the specific circumstance in each line.

The integers also have an order relation, *a is less than or equal to b* : $a \leq b$. This relation satisfies three fundamental order properties: $\leq$ is a reflexive, antisymmetric, and transitive relation on $\mathbb{Z}$.

The notation $b \geq a$ means the same as $a \leq b$. Also $a < b$ (and $b > a$) are shorthand ways to say $a \leq b$ and $a \neq b$.

The **trichotomy law** holds: for $a \in \mathbb{Z}$ exactly one of $a > 0$, $a = 0$, or $a < 0$ is true. The ordering of the integers is related to the arithmetic by several rules:

- (1) If $a < b$, then $a + c < b + c$ for all $c \in \mathbb{Z}$.
- (2) If $a < b$ and $c > 0$, then $ac < bc$.
- (3) If $a < b$ and $c < 0$, then $bc < ac$.

And, finally, the rule that justifies proofs by induction:

The Well Ordering Principle for $\mathbb{Z}$: The set of positive integers is **well-ordered**: every nonempty subset of positive integers has a least element.

Exercises

Exercise 20.1. *Prove that if $a > 0$ and $b > 0$, then $ab > 0$.*

Exercise 20.2. *Prove that if $ab = 0$, then $a = 0$ or $b = 0$. Hint: Try an indirect proof with four cases. Case 1: Show that if $a, b > 0$, then $ab \neq 0$. Case 2: Show that if $a > 0$ and $b < 0$, then $ab \neq 0$. There are two more similar cases. (This fact is called the zero divisor property.)*

Exercise 20.3. *Prove the cancellation law for multiplication: For integers a, b, c , with $c \neq 0$, if $ac = bc$, then $a = b$. (Hint: Use exercise [20.2](#))*

Problems

Problem 20.1. *Prove that if $a > 0$ and $b < 0$, then $ab < 0$.*

Problem 20.2. *Prove that if n is an integer, then $n^2 \geq 0$.*

Problem 20.3. *Prove that if $m^2 = n^2$, then $m = n$ or $m = -n$.*

(Hint from algebra: $a^2 - b^2 = (a + b)(a - b)$.)

Chapter 21: The Divides Relation and Primes

Given integers a and b we say that a **divides** b and write $a|b$ provided there is an integer c with $b = ac$. So, a divides b means a divides into b **evenly**. When a divides b we also say that a is a **factor** of b , or that a is a **divisor** of b , or that b is a **multiple** of a . For example, $3|12$ since $12 = 3 \cdot 4$. Keep in mind that *divides* is a relation. When you see $a|b$ you should think *is that true or false*. Don't write things like $3|12 = 4$. If a does not divide b , write $a \nmid b$. For example, it is true that $3 \nmid 13$ since 3 does not divide into 13 **evenly**.

Here is a list of a few simple facts about the divisibility relation.

Theorem 21.1. For $a, b, c \in \mathbb{Z}$ we have

- 1) $a|0$
- 2) $\pm 1|a$
- 3) If $a|b$, then $-a|b$.
- 4) If $a|b$ and $b|c$, then $a|c$. So, the divides relation is transitive on $\mathbb{Z}$.
- 5) $a| -a$
- 6) If $a|b$ and $b \neq 0$, then $0 < |a| \leq |b|$.
- 7) If $a|1$, then $a = \pm 1$.
- 8) If $a|b$ and $b|a$, then $a = \pm b$. So, the divides relation is not quite antisymmetric.
- 9) If $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.
- 10) If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$.

Proof. Here are proofs for some of the items in the theorem.

1): For any integer a we have $a \cdot 0 = 0$, so $a|0$.

4): Suppose that $a|b$ and $b|c$. Then there exist integers s, t so that $b = as$ and $c = bt$. Substituting as for b in the latter equation gives $c = (as)t = a(st)$. Thus $a|c$ since $st \in \mathbb{Z}$.

9): Suppose that $a|b$ and $a|c$. Then there exist integers s, t so that $b = as$ and $c = at$. Multiply the first equation by m and multiply the second equation by n to get $mb = a(sm)$ and $nc = a(nt)$. Add these two equations to arrive at $mb + nc = a(sm) + a(nt) = a(sm + nt)$. From which we conclude $a|(mb + nc)$ since $mb + nc \in \mathbb{Z}$. ■

The prime integers play a central role in number theory. A positive integer larger than 1 is said to be **prime** if its only positive divisors are 1 and itself.

The primes less than 100 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 97.

A positive integer larger than 1 which is not prime is **composite**. So, a composite number n has a positive divisor a which is neither 1 nor n . By part (6) of the theorem above, $1 < a < n$.

So, to check if an integer n is a prime, we can trial divide it by $2, 3, 4, 5, \dots, n - 1$ in turn. If we find one of these that divides n , we can stop, concluding that n is not a prime. On the other hand, if we find that none of those divide n , then we can conclude n is a prime. This algorithm for checking a number for primality can be made more efficient. For example, there is really no need to test to see if 4 divides n if we have already determined that 2 does not divide n . And the same reasoning shows that to test n for primality we need only check in to see if n is divisible by any of $2, 3, 5, 7, 11, 13$ and so on up to the largest prime less than n . For example, to test 15 for primality, we would trial divide by the six values $2, 3, 5, 7, 11, 13$. But even this improved algorithm can be made more efficient by the following theorem.

Theorem 21.2. *Every composite number n has a divisor a , with $2 \leq a \leq \sqrt{n}$.*

Proof. Suppose n is a composite integer. That means $n = ab$ where $1 < a, b < n$. Not both a and b are greater than $\sqrt{n}$, for if so $n = ab > \sqrt{n}\sqrt{n} = \sqrt{n^2} = n$. $\rightarrow \leftarrow$ ■

So, if we haven't found a divisor of n by the time we reach $\sqrt{n}$, then n must be prime.

We can be a little more informative, as the next theorem shows.

Theorem 21.3. *Every integer $n > 1$ is divisible by a prime.*

Proof. Let $n > 1$ be given. The set $D_n^+ = \{m \in \mathbb{Z} | m > 1 \wedge m|n\}$ is nonempty since $n \in D_n^+$. Let m be the least integer in D_n^+ . Then m must be prime, since if k is an integer with $1 < k < m$ and $k|m$, then $k|n$ by transitivity of the divides relation. But this contradicts the minimality of m . ■

Alternative proof. Notice that $n = 2$ has a prime divisor.

Suppose that every integer $2 \leq k < n$ has a prime divisor.

Consider the integer n . Either n is prime or n is composite. If n is prime, we are done. If n is composite it has a divisor a with $2 \leq a < n$. By inductive hypothesis a has a prime divisor. Thus by transitivity of the divides relation so does n . ■

Theorem 21.4. *The set of prime integers is infinite.*

Proof. Suppose that there were only finitely many primes. List them all: $2, 3, 5, 7, \dots, p$. Form the number $N = 1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot p$. According to the last theorem, there must be a prime that divides N , say q . Certainly q also divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot p$ since that is the product of all the primes, so q is one of its factors. Hence q divides $N - 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot p = 1$. But that's crazy since only ± 1 divide 1. Thus q cannot be prime. We have reached a contradiction, and so we can conclude there are infinitely many primes. ■

Theorem 21.5 (The Division Algorithm for Integers). *If $a, d \in \mathbb{Z}$, with $d > 0$, there exist unique integers q and r , with $a = qd + r$, and $0 \leq r < d$.*

Proof. Let $S = \{a - nd | n \in \mathbb{Z} \text{ and } a - nd \geq 0\}$. Then $S \neq \emptyset$, since $a - (-|a|)d \in S$ for sure. Thus, by the Well Ordering Principle, S has a least element, call it r . Say $r = a - qd$. Then we

have $a = qd + r$ and $0 \leq r$. If $r \geq d$, then $a = (q + 1)d + (r - d)$, with $0 \leq r - d$ contradicting the minimality of r . Therefore, $0 \leq r < d$.

To prove uniqueness, suppose that $a = q_1d + r_1 = q_2d + r_2$, with $0 \leq r_1, r_2 < d$. Collect the quotient terms and remainder terms to get $d(q_1 - q_2) = r_2 - r_1$. This implies that $r_2 - r_1$ is a multiple of d . Since $0 \leq r_1, r_2 < d$, we have $-d < r_2 - r_1 < d$. Thus, the only multiple of d which $r_2 - r_1$ can possibly be is $0 \cdot d = 0$. So $r_2 - r_1 = 0$ which is the same thing as $r_1 = r_2$. Thus $d(q_1 - q_2) = 0 = d \cdot 0$. Since $d \neq 0$ we can cancel d to get $q_1 - q_2 = 0$. Thus $q_1 = q_2$. ■

The quantities q and r in the division algorithm are called the **quotient** and **remainder** when a is divided by d .

Exercises

Exercise 21.1. Determine the quotient and remainder when 107653 is divided by 22869.

Exercise 21.2. Determine if 1297 is a prime.

Exercise 21.3. Prove or give a counterexample: The divides relation is reflexive.

Exercise 21.4. Prove or give a counterexample: The divides relation is symmetric.

Exercise 21.5. Prove or give a counterexample: The divides relation is transitive.

Exercise 21.6. What is wrong with the expression $4|12 = 3$?

Exercise 21.7. Show that none of the 1000 consecutive integers $1001! + 2$ to $1001! + 1001$ are primes.

Exercise 21.8. Prove: For $a, b \in \mathbb{Z}$, if $a|b$, then $-a|b$.

Problems

Problem 21.1. For positive integers, a and b , if the quotient when a is divided by b is q , what are the possible quotients when $a + 1$ is divided by b ?

Problem 21.2. For positive integers, a and b , if the quotient when a is divided by b is q , what are the possible quotients when $2a$ is divided by b ?

Problem 21.3. Prove or give a counterexample: If p is a prime, then $2p + 1$ is a prime.

Problem 21.4. Determine all the integers that 0 divides. (Hint: Think about the definition of the divides relation. The correct answer is probably not what you expect.)

Problem 21.5. Determine if 3599 is a prime. (Hint: This is easy since $3599 = 3600 - 1$.)

Problem 21.6. Determine if 5129 is a prime.

Problem 21.7. Prove property 10 of Theorem 21.1: For integers a, b, c , if $a|b$, then $a|bc$.

Chapter 22: GCD's and the Euclidean Algorithm

The **greatest common divisor** of a and b , not both 0, is the largest integer which divides both a and b . For example, the greatest common divisor of 21 and 35 is 7. We write $\gcd(a, b)$, as shorthand for the greatest common divisor of a and b . So $\gcd(35, 21) = 7$.

There are several ways to find the greatest common divisor of two integers, a and b (not both 0).

First, we could simply list all the positive divisors of a and b and pick the largest number that appears in both lists. Notice that 1 will appear in both lists. For the previous example the positive divisors of 35 are 1, 5, 7, and 35. For 21 the positive divisors are 1, 3, 7, and 21. The largest number appearing in both lists is 7, so $\gcd(35, 21) = 7$.

Another way to say the same thing: If we let D_a^+ denote the set of positive divisors of a , then $\gcd(a, b) =$ the largest number in $D_a^+ \cap D_b^+$.

The reason $\gcd(0, 0)$ is not defined is that every positive integer divides 0, and so there is no largest integer that divides 0. From now on, when we use the symbol $\gcd(a, b)$, we will tacitly assume a and b are not both 0. The integers a and b can be negative. For example, if $a = -34$ and $b = 14$, then the set of positive divisors of -34 is $\{1, 2, 17, 34\}$ and the set of positive divisors of 14 is $\{1, 2, 7, 14\}$. The set of positive common divisors of 14 and -34 is the set

$$\{1, 2, 17, 34\} \cap \{1, 2, 7, 14\} = \{1, 2\}.$$

The largest number in this set is $2 = \gcd(-34, 14)$.

Obviously then $\gcd(a, b) = \gcd(-a, b)$ since a and $-a$ have the same set of positive divisors. So, when computing the $\gcd(a, b)$ we may as well replace a and b by their absolute values if one or both happen to be negative.

Here are a few easy facts about greatest common divisors:

- (1) If $a \neq 0$, then $\gcd(a, a) = |a|$.
- (2) $\gcd(a, 1) = 1$.
- (3) $\gcd(a, b) = \gcd(b, a)$. (The order a and b are given is not important, but it is traditional to list them with $a \geq b$.)
- (4) If $a \neq 0$ and $a|b$, then $\gcd(a, b) = |a|$.
- (5) If $a \neq 0$, $\gcd(a, 0) = |a|$.

If $\gcd(a, b) = 1$, we say that a and b are **relatively prime**. When a and b are relatively prime, they have no common prime divisor. For example, 12 and 35 are relatively prime.

It's clear that computing $\gcd(a, b)$ by listing all the positive divisors of a and all the positive divisors of b and selecting the largest integer that appears in both lists is not very efficient. There is a better way of computing $\gcd(a, b)$.

Theorem 22.1. *If a and b are integers (not both 0) and $a = sb + t$ for integers s and t , then*

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

Proof. To prove the theorem we will show that the list of positive integers that divide both a and b is identical to the list of positive integers that divide both b and $t = a - sb$. So, suppose $d|a$ and $d|b$. Then $d|(a - sb)$ so $d|t$. Hence d divides both b and t . On the other hand, suppose $d|b$ and $d|t$. Then $d|(sb + t)$, so that $d|a$. Hence d divides both a and b . It follows that $\gcd(a, b) = \gcd(b, t)$. ■

Euclid is given the credit for discovering this fact, and its use for computing greatest common divisors is called the **Euclidean algorithm** in his honor. The idea is to use the theorem repeatedly until a pair of numbers is reached for which the greatest common divisor is obvious. Here is an example of the Euclidean algorithm in action.

Example 22.2. *Since $14 = 1 \cdot 10 + 4$, $\gcd(14, 10) = \gcd(10, 4)$. In turn $10 = 2 \cdot 4 + 2$ so $\gcd(10, 4) = \gcd(4, 2)$. Since $4 = 2 \cdot 2$, $\gcd(4, 2) = \gcd(2, 0) = 2$. So $\gcd(14, 10) = 2$.*

The same example, presented a little more compactly, and without explicitly writing out the divisions, looks like

$$\gcd(14, 10) = \gcd(10, 4) = \gcd(4, 2) = \gcd(2, 0) = 2$$

At each step, the second number is replaced by the remainder when the first number is divided by the second, and the second moves into the first spot. The process is repeated until the second number is a 0 (which must happen eventually since the second number never will be negative, and it goes down by at least 1 with each repetition of the process). The greatest common divisor is then the number in the first spot when the second spot is 0 in the last step of the algorithm.

Example 22.3. *Find the greatest common divisor of 540 and 252. We may present the computations compactly, without writing out the divisions. We have*

$$\gcd(540, 252) = \gcd(252, 36) = \gcd(36, 0) = 36.$$

The Euclidean algorithm can also be written out as a sequence of divisions:

$$\begin{aligned} a &= q_1 \cdot b + r_1, 0 < r_1 < b \\ b &= q_2 \cdot r_1 + r_2, 0 < r_2 < r_1 \\ r_1 &= q_3 \cdot r_2 + r_3, 0 < r_3 < r_2 \\ &\vdots \\ r_k &= q_{k+2} r_{k+1} + r_{k+2}, 0 < r_{k+2} < r_{k+1} \\ &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n, 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

The sequence of integer remainders $b > r_1 > \cdots > r_k > \cdots \geq 0$ must eventually reach 0. Let's say $r_n \neq 0$, but $r_{n+1} = 0$, so that $r_{n-1} = q_{n+1}r_n$. That is, in the sequence of remainders, r_n is the last non-zero term. Then, just as in the examples above we see that the greatest common divisor of a and b is the last nonzero remainder:

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n.$$

Let's find $\gcd(317, 118)$ using this version of the Euclidean algorithm. Here are the steps:

$$317 = 2 \cdot 118 + 81$$

$$118 = 1 \cdot 81 + 37$$

$$81 = 2 \cdot 37 + 7$$

$$37 = 5 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Since the last non-zero remainder is 1, we conclude that $\gcd(317, 118) = 1$. So, in the terminology introduced above, we would say that 317 and 118 are relatively prime.

Using the Euclidean algorithm to find greatest common divisors is extremely efficient. A computer implementation of the Euclidean algorithm will produce the greatest common divisor of integers of hundreds of digits in the blink of an eye. A variation using the least remainder in absolute value version of the division algorithm runs in $\mathcal{O}(\lg b)$ time.

If your instructor did not cover chapters 17 through 19 ask them about this in office hours.

Exercises

Exercise 22.1. Use the Euclidean algorithm to compute $\gcd(a, b)$ in each case.

- (a) $a = 233, b = 89$
- (b) $a = 1001, b = 13$
- (c) $a = 2457, b = 1458$
- (d) $a = 567, b = 349$

Exercise 22.2. Compute $\gcd(987654321, 123456789)$.

Exercise 22.3. Write a step-by-step algorithm that implements the Euclidean algorithm for finding greatest common divisors.

Exercise 22.4. If n is a positive integer, what is $\gcd(n, 2n)$?

Problems

Problem 22.1. Use the Euclidean algorithm to compute $\gcd(a, b)$ in each case.

- (a) $a = 216, b = 111$
- (b) $a = 1001, b = 11$
- (c) $a = 633, b = 5168$
- (d) $a = 1357, b = 2468$

Problem 22.2. Compute $\gcd(733103, 91637)$.

Problem 22.3. If p is a prime, and n is any integer, what are the possible values of $\gcd(p, n)$?

Problem 22.4. Prove or give a counterexample: If p and q are distinct primes, then $\gcd(2p, 2q) = 2$.

Problem 22.5. If p is a prime, and m is a positive integer, determine $\gcd(p, p^m)$.

Problem 22.6. If p is a prime, and $m \leq n$ are positive integers, determine $\gcd(p^n, p^m)$.

Problem 22.7. Show that if n is a positive integer, then $\gcd(n, n + 1) = 1$.

Chapter 23: GCD's Reprised

The greatest common divisor of two integers a and b , not both zero, is defined to be the largest integer $\gcd(a, b)$ that divides them both. But there is another way to describe the greatest common divisor. First, a little vocabulary: recall that a **linear combination** of a and b is any expression of the form $as + bt$ where s, t are integers. For example, $4 \cdot 5 + 10 \cdot 2 = 40$ is a linear combination of 4 and 10. Here are some more linear combinations of 4 and 10:

$$4 \cdot 1 + 10 \cdot 1 = 14, 4 \cdot 0 + 10 \cdot 0 = 0 \text{ and } 4 \cdot (-11) + 10 \cdot 1 = -34.$$

If we make a list of all possible linear combinations of 4 and 10, an unexpected pattern appears: $\dots, -6, -4, -2, 0, 2, 4, 6, \dots$. Since 4 and 10 are both even, we are sure to see only even integers in the list of linear combinations, but the surprise is that *every* even number is in the list. Now here's the connection with greatest common divisors: The greatest common divisor of 4 and 10 is 2, and the list of all linear combinations is exactly all multiples of 2. Let's prove that that was no accident.

Theorem 23.1. *Let a, b be two integers (not both zero). Then the smallest positive number in the list of the linear combinations of a and b is $\gcd(a, b)$. In other words, the $\gcd(a, b)$ is the smallest positive integer that can be written as a linear combination of a and b .*

Proof. Let $L = \{as + bt \mid s, t \text{ are integers and } as + bt > 0\}$. Since a, b are not both 0, we see this set is nonempty. As a nonempty set of positive integers, it must have a least element, say m . Since $m \in L$, m is a linear combination of a and b . Say $m = as_0 + bt_0$. We need to show that $m = \gcd(a, b) = d$.

As noted above, since $d|a$ and $d|b$, it must be that $d|(as_0 + bt_0)$, so $d|m$. That implies $d \leq m$.

We complete the proof by showing that m is a common divisor of a and b . The plan is to divide a by m and show that the remainder must be 0. So, write $a = qm + r$ with $0 \leq r < m$. Solving for r we get $0 \leq r = a - qm = a - q(as_0 + bt_0) = a(1 - qs_0) + b(-qt_0) < m$. This shows that r is a nonnegative linear combination of a and b that is less than m . Since m is the smallest positive linear combination of a and b the only option for r is 0. Thus $m|a$. By symmetry of argument $m|b$. Since m is a common divisor of a and b we have $m \leq d = \gcd(a, b)$. Because the relation $\leq$ is antisymmetric on $\mathbb{Z}$ we have $m = d$. ■

And now we are ready for the punchline.

Theorem 23.2. *Let a, b be two integers (not both zero). Then the list of all the linear combinations of a and b consists of all the multiples of $\gcd(a, b)$.*

Proof. Since $\gcd(a, b) = d$ divides any linear combination of a and b , only multiples of d can be in the set $L = \{as + bt \mid s, t \text{ are integers and } as + bt > 0\}$. Now we need to show that if n is a multiple of d , then $n \in L$. By the previous theorem $d = as_0 + bt_0$ for some integers s, t . Thus if $0 < n = kd$, then $n = k(as_0 + bt_0) = a(ks_0) + b(kt_0) \in L$. ■

So, without doing any computations, we can be sure that the set of all linear combinations of 15 and 6 will be all multiples of 3.

In practice, finding integers s and t so that $as + bt = d = \gcd(a, b)$ is carried out by using the Euclidean algorithm applied to a and b , then *back-solving*.

Example 23.3. Let $a = 35$ and $b = 55$. Then the Euclidean algorithm gives

$$55 = 1 \cdot 35 + 20$$

$$35 = 1 \cdot 20 + 15$$

$$20 = 1 \cdot 15 + 5$$

$$15 = 3 \cdot 5 + 0$$

The penultimate equation allows us to write $5 = 1 \cdot 20 + (-1) \cdot 15$ as a linear combination of 20 and 15. We then rewrite $35 = 1 \cdot 20 + 15$ as $15 = 1 \cdot 35 + (-1) \cdot 20$ and substitute to get

$$5 = 1 \cdot 20 + (-1) \cdot 15 = 1 \cdot 20 + (-1)(1 \cdot 35 + (-1) \cdot 20)$$

Collecting 20's and 35's yields $5 = (-1) \cdot 35 + 2 \cdot 20$. Finally, we rewrite $55 = 1 \cdot 35 + 20$ as $20 = 1 \cdot 55 + (-1) \cdot 35$ and substitute to get

$$5 = (-1) \cdot 35 + 2 \cdot 20 = (-1) \cdot 35 + 2(1 \cdot 55 + (-1) \cdot 35).$$

This simplifies to $5 = 2 \cdot 55 + (-3) \cdot 35$.

This sort of computation is precarious. We must treat the remainders from the Euclidean Algorithm as variables – we cannot rewrite them. But, on the whole, we are only really doing arithmetic. Also, the back-solving method is not very adaptable to writing a program to solve the problem of writing $\gcd(a, b)$ as a linear combination of a and b . A streamlined version called the continued fraction method uses forward-substitution to more easily solve the problem.

To use the continued fraction method on the example above we first build a four-row table with $6 = 2 + 4$ columns. We begin filling in the table by placing a and b in the top row left hand spaces. We put *'s below them in the second row (these entries are not used). Then we fill out the last two rows of the first two columns as shown.

55	35				
*	*				
0	1				
1	0				

We complete the first row by using the remainders from the Euclidean Algorithm.

$$55 = 1 \cdot 35 + 20$$

$$35 = 1 \cdot 20 + 15$$

$$20 = 1 \cdot 15 + 5$$

$$15 = 3 \cdot 5 + 0$$

55	35	20	15	5	0
*	*				
0	1				
1	0				

We complete the second row by using the quotients from the Euclidean Algorithm.

$$55 = 1 \cdot 35 + 20$$

$$35 = 1 \cdot 20 + 15$$

$$20 = 1 \cdot 15 + 5$$

$$15 = 3 \cdot 5 + 0$$

55	35	20	15	5	0
*	*	1	1	1	3
0	1				
1	0				

Finally, the remaining entries in each of the bottom two rows are filled in one after the other from left to right by taking the quotient entry in a column times the row entry one column back and then adding the row entry two columns back. For example, to compute the c in the following table use $c = q \cdot j + k$.

*	*			q	
0	1	k	j	c	
1	0				

Using that rule to complete the table for 55 and 35 we obtain the result

55	35	20	15	5	0
*	*	1	1	1	3
0	1	1	2	3	11
1	0	1	1	2	7

We don't need the bottom two entries in the last column. But observe that $7 \cdot 55 = 11 \cdot 35$. This will always be true! So, we have a nice way to check that we have correctly filled out the table.

Anyway we now find integers s and t so that $\gcd(a, b) = s \cdot a + t \cdot b$. Obviously one of s and t will be positive and the other negative - but which one? The answer lies in counting the number

of back-substitutions we would have made. Start with a $+$ at the one in the first column of the bottom row, and step along alternating $+$ and $-$ in each column. This will give the correct sign for s which is the second to last entry in the bottom row. The sign of t is the opposite and the absolute value of t is the entry in the 3rd row and second to last column.

In our running example we have $s = +2$ and $t = -3$ and can check that

$$5 = \gcd(55, 35) = 2 \cdot 55 + (-3) \cdot 35.$$

In general, to use the continued fraction table method to write $\gcd(a, b) = s \cdot a + t \cdot b$ we build a table with four rows and $n + 2$ columns, where the Euclidean Algorithm applied to a and b requires n steps and $r_n = 0$. In practice, as noticed above, we can omit the last column.

Exercises

Exercise 23.1. Determine $\gcd(13447, 7667)$ and write it as a linear combination of 13447 and 7667. Try both the method of back-substitution and the Extended Euclidean Algorithm to determine a suitable linear combination.

Exercise 23.2. What can you conclude about $\gcd(a, b)$ if $as + bt = 1$ for some integers s, t ?

Exercise 23.3. What can you conclude about $\gcd(a, b)$ if $as + bt = 19$ for some integers s, t ?

Exercise 23.4. What can you conclude about $\gcd(a, b)$ if $as + bt = 18$ for some integers s, t ?

Problems

Problem 23.1. Determine $\gcd(41559, 39417)$ and write it as a linear combination of 41559 and 39417. Try both the method of back-substitution and the Extended Euclidean Algorithm to determine a suitable linear combination.

Problem 23.2. What can you conclude about $\gcd(a, b)$ if $as + bt = 12$ for some integers s, t ?

Problem 23.3. What is the smallest positive integer that can be written as a linear combination of 2191 and 1351?

Problem 23.4. Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b .

Example: the least common multiple of 24 and 18 is 72. Write that as $\text{lcm}(24, 18) = 72$.

You might recall the notion of least common multiple from the time you learned how to add fractions. The idea was that to add two fractions, $\frac{a}{b}$ and $\frac{c}{d}$, first write the two as equivalent fractions with the same denominator. For example, to add $\frac{2}{3}$ and $\frac{5}{4}$, write them as $\frac{8}{12}$ and $\frac{15}{12}$, then add to get $\frac{23}{12}$. The least common denominator when adding $\frac{a}{b}$ and $\frac{c}{d}$ is the least common multiple of the denominators, $\text{lcm}(b, d)$.

Determine $\text{lcm}(22, 33)$. (The answer is not 726.)

Problem 23.5. The result when $\gcd(a, b)$ and $\text{lcm}(a, b)$ are multiplied is always a simple combination of a and b . Example: $\gcd(6, 4) \cdot \text{lcm}(6, 4) = 2 \cdot 12 = 24$. Try a few more examples and see if you can guess the value of $\gcd(a, b) \cdot \text{lcm}(a, b)$.

Chapter 24: The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states the familiar fact that every positive integer greater than 1 can be written in exactly one way as a product of primes. For example, the prime factorization of 60 is $2^2 \cdot 3 \cdot 5$, and the prime factorization of 625 is 5^4 . The factorization of 60 can be written in several different ways: $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 \cdot 2$, and so on. The order in which the factors are written does not matter. The factorization of 60 into primes will always have two 2's, one 3, and one 5. One more example: The factorization of 17 consists of the single factor 17. In the *standard form* of the factorization of an integer greater than 1, the primes are written in order of size, and exponents are used for primes that are repeated in the factorization. So, for example, the standard factorization of 60 is $60 = 2^2 \cdot 3 \cdot 5$.

Before proving the Fundamental Theorem of Arithmetic, we will need to assemble a few facts.

Theorem 24.1 (Euclid's Lemma). *If $n|ab$ and n and a are relatively prime, then $n|b$.*

Proof. Suppose that $n|ab$ and $\gcd(n, a) = 1$. We can find integers s, t, k so that $ns + at = 1$ and $ab = nk$. Multiply both sides of the equation $ns + at = 1$ by b to get $nsb + abt = b$. Now substitute nk for ab and factor an n out to get $n(sb + kt) = b$. Since $sb + kt \in \mathbb{Z}$ we deduce that n divides b . ■

One consequence of this theorem is that if a prime divides a product of some integers, then it must divide one of the factors. That is so since if a prime does not divide an integer, then it is relatively prime to that integer. That is useful enough to state as a theorem.

Theorem 24.2. *If p is a prime, and $p|a_1a_2 \dots a_n$, then $p|a_j$ for some $j = 1, 2, \dots, n$.*

Theorem 24.3 (Fundamental Theorem of Arithmetic). *If $n > 1$ is an integer, then there exist prime numbers $p_1 \leq p_2 \leq \dots \leq p_r$ such that $n = p_1p_2 \dots p_r$ and there is only one such prime factorization of n .*

Proof. There are two things to prove: (1) every $n > 1$ can be written in at least one way as a product of primes (in increasing order) and (2) there cannot be two different such expressions equal to n .

We will prove these by induction. For the basis, we see that 2 can be written as a product of primes (namely $2 = 2$) and, since 2 is the smallest prime, this is the only way to write 2 as a product of primes.

For the inductive step, suppose every integer from 2 to k can be written uniquely as a product of primes. Now consider the number $k + 1$. We consider two cases:

Case 1: If $k + 1$ is a prime, then $k + 1$ is already an expression for $k + 1$ as a product of primes. There cannot be another expression for $k + 1$ as a product of primes. For if $k + 1 = pm$ with p a prime, then $p|k + 1$. Since p and $k + 1$ are both prime that tells us $p = k + 1$ and $m = 1$.

Case 2: If $k + 1$ is not a prime, then we can write $k + 1 = ab$ with $2 \leq a, b \leq k$. By the induction hypothesis each of a and b can be written as products of primes. Say $a = p_1 \dots p_s$ and

$b = q_1 \dots q_t$. That means that $k + 1 = p_1 \dots p_s q_1 \dots q_t$ and we can re-arrange the primes in increasing order.

It remains to show that $k + 1$ cannot be written in more than one way as a product of an increasing list of primes. Let's suppose that $k + 1 = u_1 u_2 \dots u_l = v_1 v_2 \dots v_m$ where the u_i s and v_j s are primes listed in increasing order. Since u_1 divides $v_1 v_2 \dots v_m$ it must divide one of the v_i s. Since u_1 and v_i are primes, $u_1 | v_i$ implies $u_1 = v_i$. Since the v_i s are in increasing order we know $u_1 \geq v_1$. By symmetry of argument, we know $v_1 \geq u_1$. Thus $u_1 = v_1$ (i.e. $v_i = v_1$). We can cancel u_1 from both sides of $u_1 u_2 \dots u_l = v_1 v_2 \dots v_m$ to deduce $u_2 \dots u_l = v_2 \dots v_m$. Each side of $u_2 \dots u_l = v_2 \dots v_m$ is now a different factorization of an integer smaller than $k + 1$. This contradicts the induction hypothesis. $\rightarrow \leftarrow$ ■

We can apply the Fundamental Theorem of Arithmetic to the problem of counting the number of positive divisors of an integer greater than 1. For example, consider the integer $12 = 2^2 3$. It follows from the Fundamental Theorem that the positive divisors of 12 must look like $2^a 3^b$ where $a = 0, 1, 2, b = 0, 1$. So, there are six positive divisors of 12:

$$2^0 3^0 = 1, 2^1 3^0 = 2, 2^2 3^0 = 4, 2^0 3^1 = 3, 2^1 3^1 = 6 \text{ and } 2^2 3^1 = 12.$$

Exercises

Exercise 24.1. Determine the prime factorization of 345678.

Exercise 24.2. Determine the prime factorization of 1016.

Exercise 24.3. List all the positive divisors of 1016.

Exercise 24.4. How many positive divisors does 345678 have?

Problems

Problem 24.1. Determine the prime factorization of 13579.

Problem 24.2. List all the positive divisors of 13579.

Problem 24.3. Prove that if n is an even integer bigger than 2, then $2^n - 1$ is not a prime. Examples: $2^4 - 1 = 15 = (3)(5)$, $2^{10} - 1 = 1023 = (3)(11)(31)$, and Hint: Recall the factorization from college algebra $s^2 - t^2 = (s + t)(s - t)$.

Problem 24.4. Prime factorizations can be used to find greatest common divisors and least common multiples. The method is very inefficient compared to the Euclidean Algorithm since there is no known fast method of finding prime factorizations. Suppose a and b are two positive integers. Factor them each as product of primes. Say

$$a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \text{ and } b = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}.$$

Note that the same list of primes is used for both factorizations, so we will need to allow exponents to be 0 or more. For example, for $a = 12$ and $b = 15$ we write $a = 12 = 2^2 \cdot 3^1 \cdot 5^0$ and $15 = 2^0 \cdot 3^1 \cdot 5^1$.

Prove: $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}.$

Example: $\gcd(12, 15) = 2^{\min(2, 0)} 3^{\min(1, 1)} 5^{\min(0, 1)} = 2^0 3^1 5^0 = 3.$

Prove: $\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_n^{\max(e_n, f_n)}.$

Example: $\text{lcm}(12, 15) = 2^{\max(2, 0)} 3^{\max(1, 1)} 5^{\max(0, 1)} = 2^2 3^1 5^1 = 60.$

Problem 24.5. Using the formulas for greatest common divisor and least common multiple in the previous two problems, prove the result you guessed in the last chapter for the product of $\gcd(a, b) \text{lcm}(a, b)$. (Hint: The fact you need is $\min(s, t) + \max(s, t) = s + t$, which is not hard to prove.)

Chapter 25: Linear Diophantine Equations

Consider the following problem:

Al buys some books at \$25 each, and some magazines at \$3 each. If he spent a total of \$88, how many books and how many magazines did Al buy? At first glance, it does not seem we are given enough information to solve this problem. Letting x be the number of books Al bought, and y the number of magazines, then the equation we need to solve is $25x + 3y = 88$. Thinking back to college algebra days, we recognize $25x + 3y = 88$ as the equation of a straight line in the plane, and any point along the line will give a solution to the equation. For example, $x = 0$ and $y = 88/3$ is one solution. But, in the context of this problem, that solution makes no sense because Al cannot buy a fraction of a magazine. We need a solution in which x and y are both integers. In fact, we need even a little more care than that. The solution $x = -2$ and $y = 46$ is also unacceptable since Al cannot buy a negative number of books. So, we really need solutions in which x and y are both nonnegative integers. The problem can be solved by brute force: If $x = 0$, y is not an integer. If $x = 1$, then $y = 21$, so that is one possibility. If $x = 2$, y is not an integer. If $x = 3$, y is not an integer. And, if x is 4 or more, then y would have to be negative. So, it turns out there is only one possible solution: Al bought one book, and 21 magazines.

The above question is an example of a Diophantine problem. Pronounce Diophantine as *dee-uh-FAWN-teen* or *dee-uh-FAWN-tine*, or, the more common variations, *die-eh-FAN-teen* or *die-eh-FAN-tine*.

<http://www.merriam-webster.com/audio.php?file=diopha01&word=Diophantineequation>

For a modern pronunciation of Diophantus's name ($\Delta\iota\phi\alpha\nu\tau\omicron\zeta$) see

<http://www.pronouncenames.com/Diophantus>. In general, problems in which we are interested in finding solutions in which the variables are to be integers are called **Diophantine** problems.

In this chapter we will learn how to easily find the solutions to all linear Diophantine equations: $ax + by = c$ where a, b, c are given integers. To show some of the subtleties of such problems, here are two more examples:

- (1) Al buys some book Al buys some books at \$24 each, and some magazines at \$3 each. If he spent a total of \$875, how many books and how many magazines did Al buy? For this question we need to solve the Diophantine equation $24x + 3y = 875$. In this case there are no possible solutions. For any integers x and y , the left-hand side will be a multiple of 3 and so cannot be equal to 875 which is not a multiple of 3.
- (2) Al buys some books at \$26 each, and some magazines at \$3 each. If he spent a total of \$157, how many books and how many magazines did Al buy? Setting up the equation as before, we need to solve the Diophantine equation $26x + 3y = 157$. A little trial and error, testing $x = 0, 1, 2, 3$, and so on shows there are two possible answers this time: $(x, y) \in \{(2, 35), (5, 9)\}$.

Determining all the solutions to $ax + by = c$ is closely connected with the idea of greatest

common divisors. One connection is theorem [23.2](#). Here is how solutions of $ax + by = c$ are related.

Theorem 25.1. $ax + by = c$ has a solution in the integers if and only if $\gcd(a, b)$ divides c .

So, for example, $9x + 6y = 211$ has no solutions (in the integers) while $9x + 6y = 213$ does have solutions. To find a solution to the last equation, apply the Extended Euclidean Algorithm method to write the $\gcd(9, 6)$ as a linear combination of 9 and 6 (actually, this one is easy to do by sight): $9 \cdot 1 + 6 \cdot (-1) = 3$, then multiply both sides by $\frac{213}{\gcd(9, 6)} = \frac{213}{3} = 71$ to arrive at $(71) \cdot 9 + (-71) \cdot 6 = 213$. That shows $x = 71, y = -71$ is a solution to $9x + 6y = 213$.

But that is only one possible solution. When a linear Diophantine equation has one solution it will have infinitely many. In the example above, another solution will be $x = 49$ and $y = -38$. Checking shows that $(49) \cdot 9 + (-38) \cdot 6 = 213$.

There is a simple recipe for all solutions, once we have found one particular solution.

Theorem 25.2. Let $d = \gcd(a, b)$. Suppose $x = s$ and $y = t$ is one solution to $ax + by = c$. Then all solutions are given by

$$x = s + k \left(\frac{b}{d} \right) \text{ and } y = t - k \left(\frac{a}{d} \right) \text{ where } k \text{ is any integer.}$$

Proof. It is easy to check that all the displayed x, y pairs are solutions simply by plugging in:

$$a \left(s + k \left(\frac{b}{d} \right) \right) + b \left(t - k \left(\frac{a}{d} \right) \right) = as + \frac{abk}{d} + bt - \frac{abk}{d} = as + bt = c.$$

Checking that the displayed formulas for x and y give all possible solutions is trickier. Let's assume $a \neq 0$. Suppose $x = u$ and $y = v$ is a solution. That means $au + bv = c = as + bt$. It follows that $a(u - s) = b(t - v)$. Divide both sides of that equation by d to get

$$\frac{a}{d}(u - s) = \frac{b}{d}(t - v).$$

That equation shows that $\frac{a}{d} \mid \frac{b}{d}(t - v)$. Since a/d and b/d are relatively prime, we conclude that a/d divides $(t - v)$. Let's say $k \left(\frac{a}{d} \right) = t - v$. Rearrange that equation to get $v = t - k \left(\frac{a}{d} \right)$.

Next, replacing $t - v$ in the equation $\frac{a}{d}(u - s) = \frac{b}{d}(t - v)$ with $k \left(\frac{a}{d} \right)$ gives

$$\frac{a}{d}(u - s) = \frac{b}{d}(t - v) = \frac{b}{d} \left(k \frac{a}{d} \right).$$

Since $a/d \neq 0$, we can cancel that factor. So we have

$$u - s = k \left(\frac{b}{d} \right) \text{ so that } u = s + k \left(\frac{b}{d} \right). \blacksquare$$

Example 25.3. Determine all the solutions to $221x + 91y = 39$.

Using the Extended Euclidean Algorithm method, we learn that $\gcd(221, 91) = 13$ and since $13|39$, the equation will have infinitely many solutions. The Extended Euclidean Algorithm table provides a linear combination of 221 and 91 equal to 13 namely $221(-2) + 91(5) = 13$. Multiply both sides by 3 and we get $221(-6) + 91(15) = 39$. So, a particular solution to $221x + 91y = 39$ is $x = -6$, $y = 15$. According to theorem 25.2, all solutions are given by

$$x = -6 + k \frac{91}{13} = -6 + 7k \text{ and } y = 15 - k \frac{221}{13} = 15 - 17k,$$

where k is any integer.

Example 25.4. Armand is old. Armand buys some books for \$25 each and some CDs for \$12 each. If he spent a total of \$331, how many books and how many CDs did he buy?

Let x = the number of books, and y = the number of CDs. We need to solve $25x + 12y = 331$. The greatest common divisor of 25 and 12 is 1, and there is an obvious linear combination of 25 and 12 which equals 1 namely $25(1) + 12(-2) = 1$. Multiplying both sides by 331 gives $25(331) + 12(-662) = 331$. So a particular solution to $25x + 12y = 331$ is $x = 331$ and $y = -662$. That won't do for an answer to the given problem since we want $x, y \geq 0$. To find the suitable choices for x and y , let's look at all solutions to $25x + 12y = 331$. We have that

$$x = 331 + 12k \text{ and } y = -662 - 25k.$$

We want x and y to be at least 0, and so we need

$$331 + 12k \geq 0 \text{ and } -662 - 25k \geq 0.$$

Which means that

$$k \geq -\frac{331}{12} \text{ and } k \leq -\frac{662}{25}, \text{ or } -\frac{331}{12} \leq k \leq -\frac{662}{25}.$$

The only option for k is $k = -27$. So, we see that Armand bought $x = 331 + 12 \cdot (-27) = 7$ books and $y = -662 - 25 \cdot (-27) = 13$ CDs.

Exercises

Exercise 25.1. Find all integer solutions to $21x + 48y = 8$.

Exercise 25.2. Find all integer solutions to $21x + 48y = 9$.

Exercise 25.3. Find all integer solutions to $33x + 12y = 7$.

Exercise 25.4. Find all integer solutions to $33x + 12y = 6$.

Exercise 25.5. Sal sold some ceramic vases for \$59 each, and a number of bowls for \$37 each. If she took in a total of \$4270, how many of each item did she sell?

Problems

Problem 25.1. Find all integer solutions to $14x + 77y = 69$.

Problem 25.2. Find all integer solutions to $14x + 77y = 70$.

Problem 25.3. Beth stocked her video store with a number of video game machines at \$79 each, and a number of video games at \$41 each. If she spent a total of \$6358, how many of each item did she purchase?

Problem 25.4. If you all you have are dimes and quarters, in how many ways can you pay a \$7 bill? (For example, one way would be 10 dimes and 24 quarters.)

Problem 25.5. How many integer solutions are there to the equation $11x + 7y = 137$ if the value of x has to be at least -15 and not more than 20.

Problem 25.6. Determine all integer solutions to $5x - 7y = 99$. (Watch that minus sign!)

Chapter 26: Modular Arithmetic

Karl Friedrich Gauss made the important discovery of modular arithmetic. Modular arithmetic is also called *clock arithmetic*, and we are used to doing modular arithmetic *all the time* (pun intended). For example, consider the question *If it is 7 o'clock now, what time will it be in 8 hours?* Of course, the answer is 3 o'clock, and we found the answer by adding $7 + 8 = 15$, and then subtracting 12 to get $15 - 12 = 3$. We are so accustomed to that sort of calculation, we probably just immediately blurt out the answer without stopping to think how we figured it out. But trying a less familiar version of the same sort of problem makes it plain exactly what we needed to do to answer such questions: *If it is 7 o'clock now, what time will it be in 811 hours?* To find out, we add $7 + 811 = 818$, then divide that by 12, getting $818 = 68 \cdot 12 + 2$, and so we conclude it will be 2 o'clock. The general rule is: to find the time h hours after t o'clock, add $h + t$, divide by 12 and take the remainder.

There is nothing special about the number 12 in the above discussion. We can imagine a clock with any integer number of hours (greater than 1) on the clock. For example, consider a clock with 5 hours. What time will it be 61 hours after 2 o'clock. Since $61 + 2 = 63 = 12 \cdot 5 + 3$, the answer is 3 o'clock.

In the general case, if we have a clock with m hours, then the time h hours after t o'clock will be the remainder when $t + h$ is divided by m . So it is 2 o'clock 811 hours after 7 o'clock because $t + 811 + 7$ leaves a remainder of 2 after division by 12.

This can all be expressed in more mathematical sounding language. The key is obviously the notion of remainder. That leads to the following definition:

Definition 26.1. Given an integer $m > 1$, we say that two integers a and b are **congruent modulo m** , and write $a \equiv b \pmod{m}$, in case a and b leave the same remainder when divided by m .

Theorem 26.2. *Congruence modulo m defines an equivalence relation on $\mathbb{Z}$.*

Proof. The relation is clearly reflexive since every number leaves the same remainder as itself when divided by m . Next, if a and b leave the same remainder when divided by m , so do b and a , so the relation is symmetric. Finally, if a and b leave the same remainder, and b and c leave the same remainder, then a and c leave the same remainder, and so the relation is transitive. ■

There is an alternative way to think of congruence modulo m .

Theorem 26.3. $a \equiv b \pmod{m}$ if and only if $m|(a - b)$.

Proof. Suppose $a \equiv b \pmod{m}$. That means a and b leave the same remainder, say r when divided by m . So we can write $a = jm + r$ and $b = km + r$. Subtracting the second equation from the first gives $a - b = (jm + r) - (km + r) = jm - km = (j - k)m$, and that shows $m|(a - b)$.

For the converse, suppose $m|(a - b)$. Divide a and b by m to get the quotients and remainders: $a = jm + r$ and $b = km + s$, where $0 \leq r, s < m$. We need to show that $r = s$. Subtract the

second equation from the first to get $a - b = m(j - k) + (r - s)$. Since m divides $a - b$ and m divides $m(j - k)$, we can conclude m divides $(a - b) - m(j - k) = r - s$. Now since $0 \leq r, s < m$, the quantity $r - s$ must be one of the numbers

$$m - 1, m - 2, \dots, 2, 1, 0, -1, -2, \dots, -(m - 1).$$

The only number in that list that m divides is 0. So, $r - s = 0$, i.e. $r = s$. ■

The equivalence class of an integer a with respect to congruence modulo m will be denoted by $[a]$, or $[a]_m$ in case we are employing more than one number m as a *modulus*. In other words, $[a]$ is the set of all integers that leave the same remainder as a when divided by m . Another way to say the same thing, $[a]$ comprises all integers b such that $b - a$ is a multiple of m . That means $b - a = km$, or $b = a + km$.

That last version is often the easiest way to think about the integers that appear in $[a]$: start with a and add and subtract any number of m 's. For example, the equivalence class of 7 modulo 11 would be

$$[7] = \{\dots, -15, -4, 7, 18, 29, 40, \dots\}.$$

We know that the distinct equivalence classes partition $\mathbb{Z}$. Since dividing an integer by m leaves one of $0, 1, 2, \dots, m - 1$ as a remainder, we can conclude that there are exactly m equivalence classes modulo m . In particular, $[0], [1], [2], [3], \dots, [m - 1]$ is a list of all the distinct equivalence classes modulo m . It is traditional when working with modular arithmetic to drop the $[]$ symbols denoting the equivalence classes and simply write the representatives. So, we would say, modulo m , there are m numbers: $0, 1, 2, 3, \dots, m - 1$. But keep in mind that each of those numbers really represents a set, and we can replace any number in that list with another equivalent to it modulo m . For example, we can replace the 0 by m . The list $1, 2, 3, \dots, m - 1, m$ still consists of all the distinct values modulo m .

One reason the relation of congruence modulo m useful is that addition and multiplication of numbers modulo m acts in many ways just like arithmetic with ordinary integers.

Theorem 26.4. *If $a \equiv c \pmod{m}$, and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$ and $ab \equiv cd \pmod{m}$.*

Proof. Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then there exist integers k and l with $a = c + km$ and $b = d + lm$. So, $a + b = c + km + d + lm = (c + d) + (k + l)m$. This can be rewritten as $(a + b) - (c + d) = (k + l)m$, where $k + l$ is an integer. Therefore we have $a + b \equiv c + d \pmod{m}$. The other part is done similarly. ■

Example 26.5. *What is the remainder when $1103 + 112$ is divided by 11? We can answer this problem in two different ways. We could add 1103 and 112 and then divide by 11. Or, we could determine the remainders when each of 1103 and 112 is divided by 11, then add those remainders before dividing by 11. The last theorem promises us the two answers will be the same. In fact, $1103 + 112 = 1215 = 11 \cdot 110 + 5$ so $1103 + 112 \equiv 5 \pmod{11}$. On the other hand $1103 = 11 \cdot 100 + 3$ and $112 = 11 \cdot 10 + 2$, so that*

$$1103 + 112 \equiv 3 + 2 \equiv 5 \pmod{11}.$$

Example 26.6. *A little more impressive is the same sort of problem with operation of multiplication: what is the remainder when $1103 \cdot 112$ is divided by 11? The calculation looks like $1103 \cdot 112 \equiv 3 \cdot 2 \equiv 6 \pmod{11}$.*

Example 26.7. *For a really awe-inspiring example, let's find the remainder when 1103^{112} is divided by 11. In other words, we want to find $x = 0, 1, 2, \dots, 10$ so that*

$$1103^{112} \equiv x \pmod{11}.$$

Now 1103^{112} is a pretty big number (in fact, since $\log 1103^{112} = 112 \log 1103 \cong 340.7$ the number has 341 digits). In order to solve this problem, let's start by thinking small: Let's compute 1103^n , for $n = 1, 2, 3, \dots$.

$$1103^1 \equiv 3 \pmod{11}$$

$$1103^2 \equiv 3^2 \equiv 9 \pmod{11}$$

$$1103^3 \equiv 1103^1 \cdot 1103^2 \equiv 3 \cdot 9 \equiv 27 \equiv 5 \pmod{11}$$

$$1103^4 \equiv 1103^1 \cdot 1103^3 \equiv 3 \cdot 5 \equiv 15 \equiv 4 \pmod{11}$$

$$1103^5 \equiv 1103^1 \cdot 1103^4 \equiv 3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$$

Now that last congruence equation is very interesting. It says that whenever we see 1103^5 we may just as well write 1 if we are working modulo 11. And now we see there is an easy way to determine 1103^{112} modulo 11:

$$1103^{112} \equiv 1103^{5 \cdot 22 + 2} \equiv (1103^5)^{22} \cdot 1103^2 \equiv 1^{22} \cdot 9 \equiv 9 \pmod{11}.$$

The sort of computation in example [26.7](#) appears to be just a curiosity, but in fact the last sort of example forms the basis of one version of public key cryptography. Computations of exactly that type (but with much larger integers) are made whenever you log into a secure Internet site. It's reasonable to say that e-commerce owes its existence to the last theorem.

While modular arithmetic in many ways behaves like ordinary arithmetic, there are some differences to watch for. One important difference is the familiar *rule of cancellation*: in ordinary arithmetic, if $ab = ac$ and $a \neq 0$, then $b = c$. This rule fails in modular arithmetic. For example, $3 \not\equiv 0 \pmod{6}$ and $3 \cdot 5 \equiv 3 \cdot 7 \pmod{6}$, but $5 \not\equiv 7 \pmod{6}$.

Solving congruence equations is a popular sport. Just as with regular arithmetic with integers, if we want to solve $a + x \equiv b \pmod{m}$, we can simply set $x \equiv b - a \pmod{m}$. So, for example, solving $55 + x \equiv 11 \pmod{6}$ we would get

$$x \equiv 11 - 55 \equiv -44 \equiv 4 \pmod{6}.$$

Equations involving multiplication, such as $ax \equiv b \pmod{m}$, are much more interesting. If the modulus m is small, equations of this sort can be solved by trial-and-error: simply try all possible choices for x . For example, testing $x = 0, 1, 2, 3, 4, 5, 6$ in the congruence equation $4x \equiv 5 \pmod{7}$, we see $x \equiv 3 \pmod{7}$ is the only solution. The equation $4x \equiv 5 \pmod{8}$ has no solutions at all. And the equation $2x \equiv 4 \pmod{6}$ has $x \equiv 2, 5 \pmod{6}$ for solutions.

Theorem 26.8. *Let $d = \gcd(a, m)$. The congruence $ax \equiv b \pmod{m}$ can be solved for x if and only if $d \mid b$. In case $d \mid b$, and x_0 is one solution, there are exactly d inequivalent solutions modulo m . All solutions have the form $x_0 + k \left(\frac{m}{d}\right)$, where $k \in \mathbb{Z}$.*

Proof: We hope to write $ax \equiv b \pmod{m}$ for some integer x . So, we need m to divide the quantity $b - ax$. Thus, there is an integer k so that $b - ax = km$. Equivalently we see that $b = ax + km$ is a linear combination of a and m . Thus we need d to divide b .

To find a solution when d divides b first write $d = as + tm$ and $b = dg$ for integers s, t, g . Then $b = dg = (as + tm)g \equiv asg + tmg \equiv asg \pmod{m}$, so we take $x_0 \equiv sg \pmod{m}$.

If y is another solution we recall that if $a = df$ and $m = dh$, then $\gcd(f, h) = 1$. Now

$$ay \equiv ax_0 \equiv b \pmod{m} \text{ implies } lm = ldh = ay - ax_0 = a(y - x_0) = df(y - x_0).$$

Cancelling d we get $lh = f(y - x_0)$ i.e. h divides $f(y - x_0)$. Since $\gcd(h, f) = 1$, then h divides $y - x_0$. Thus, there is an integer e so that $y - x_0 = eh = e \left(\frac{m}{d}\right)$. This is equivalent to $y = x_0 + e \left(\frac{m}{d}\right)$ for some integer e .

To finish, two solutions $y = x_0 + k_1h$ and $z = x_0 + k_2h$ are congruent modulo m if and only if y and z differ by a multiple of m . This is if and only if there is an integer l so that $lm = ldh = z - y = k_2h - k_1h = (k_2 - k_1)h$.

This is equivalent to $k_2 - k_1 = ld$, i.e. $k_2 \equiv k_1 \pmod{d}$. ■

This constructive existence theorem yields an algorithm for solving $ax \equiv b \pmod{m}$ for x :

1. Compute $d = \gcd(a, m)$
2. If d does not divide b output “No solution” and STOP.
3. Else write $b = dg$
4. Write $d = as + tm$ (ala chapter 23)
5. Put $x_0 = (sg \pmod{m})$

Output d solutions $x_k \equiv x_0 + k \left(\frac{m}{d}\right)$, $k = 0, 1, 2, \dots, d - 1$ and STOP.

Example 26.9. *Let's find all the solutions to $2x \equiv 4 \pmod{6}$. Since $x = 2$ is an obvious solution, we see all solutions are given by $x = 2 + k\frac{6}{2} = 2 + 3k$, where k is any integer. When $k = 0, 1$ we get $x = 2, 5$. Other values of k repeat these two modulo 6. Looking at the solutions written as $x = 2 + 3k$, we see could also express the solutions as $x \equiv 2 \pmod{3}$.*

Example 26.10. *Find all solutions to $42x \equiv 35 \pmod{91}$.*

We compute $\gcd(91, 42) = 7$ and, since $7|35$, the equation will have 7 incongruent solutions modulo 91. To find one solution we write $42 \cdot (-2) + 1 \cdot 91 = 7$ and $35 = 7 \cdot 5$. So, in the algorithm above $a = 42, m = 91, s = -2, b = 35$, and $g = 5$. Thus $x_0 \equiv -10 \pmod{91}$.

The quantity $m/d = 13$ so we add multiples of 13 repeatedly to find that the solution set is

$$\dots, -23, -10, 3, 16, 29, 42, 55, 68, 81, 94, \dots$$

We select the numbers between 0 and 90 on this list:

$$3, 16, 29, 42, 55, 68, 81.$$

Exercises

Exercise 26.1. *Answer the following timing questions:*

- a) *On a military (24-hour) clock, what time is it 3122 hours after 16 hundred hours?*
- b) *What day of the week is it 3122 days after a Monday?*
- c) *What month is it 3122 months after November?*

Exercise 26.2. *List the integers in $[7]_{11}$.*

Exercise 26.3. *In a listing of the five equivalence classes modulo 5, four of the values are 1211, 218, -100 , and -3333 . What are the possible choices for the fifth value?*

Exercise 26.4. *Determine n between 0 and 24 such that $2311 + 3912 \equiv n \pmod{25}$.*

Exercise 26.5. *Determine n between 0 and 24 such that $2311 \cdot 3912 \equiv n \pmod{25}$.*

Exercise 26.6. *Determine n between 0 and 8 such that $1111^{2222} \equiv n \pmod{9}$.*

Exercise 26.7. *Solve: $4x \equiv 3 \pmod{7}$.*

Exercise 26.8. *Solve $11x \equiv 8 \pmod{57}$.*

Exercise 26.9. *Solve: $14x \equiv 3 \pmod{231}$.*

Exercise 26.10. *Solve $8x \equiv 16 \pmod{28}$.*

Exercise 26.11. *Solve: $91x \equiv 189 \pmod{231}$.*

Problems

Problem 26.1. Suppose we have a 52-card deck with the cards in order ace, 2, ..., queen, king for clubs, then diamonds, then hearts, then spades from top to bottom. A step consists of taking the top card and moving it to the bottom of the deck. We start with the ace of clubs as the top card. After two steps, the top card is the 3 of clubs. What is the top card after 735 steps?

Problem 26.2. The marks on a combination lock are numbered 0 to 39. If the lock is at mark 19, and the dial is turned one mark clockwise, it will be at mark 18. If the lock is at mark 19 and turned 137 marks clockwise at what mark will it be?

Problem 26.3. List the integers in $[11]_7$.

Problem 26.4. Arrange the numbers $-39, -27, -8, 11, 37, 68, 91$ so they are in the order $0, 1, 2, 3, 4, 5, 6$ modulo 7.

Problem 26.5. Determine n between 0 and 16 such that $311 + 891 \equiv n \pmod{17}$.

Problem 26.6. Determine n between 0 and 16 such that $(405)(777) \equiv n \pmod{17}$.

Problem 26.7. Determine n between 0 and 16 such that $710^{447} \equiv n \pmod{17}$.

Problem 26.8. Solve: $3x \equiv 5 \pmod{8}$.

Problem 26.9. Solve: $13x \equiv 12 \pmod{68}$.

Problem 26.10. Solve: $15x \equiv 12 \pmod{27}$.

Problem 26.11. Solve: $12x \equiv 9 \pmod{88}$.

Problem 26.12. Solve: $33x \equiv 183 \pmod{753}$.

Problem 26.13. Determine the unique value of n between 0 and 55 so that $n \equiv 6 \pmod{7}$ and $n \equiv 1 \pmod{8}$.

Problem 26.14. There is exactly one n between 0 and 19548 such that $n \equiv 22 \pmod{173}$ and $n \equiv 80 \pmod{113}$. Determine that n .

Chapter 27: Integers in Other Bases

The usual way of writing integers is in terms of groups of ones (units), and groups of tens, and groups of tens of tens (hundreds), and so on. Thus 237 stands for 7 units plus 3 tens and 2 hundreds, or $2 \cdot 10^2 + 3 \cdot 10 + 7$. This is the familiar decimal notation for numbers (deci = ten). But there is really nothing special about the number ten here, and it could be replaced by any integer bigger than one. That is, we could use 7 the way 10 was used above to describe a number. Thus, we would specify how many units, how many 7's and 7^2 's and 7^3 's, and so on are needed to make up the number. When a number is expressed in this fashion with b in place of the 10, the result is called the **base- b** expansion (or **radix- b** expansion) of the integer.

For example, the decimal integer 132, is made up of two 7^2 's, four 7's and finally six units. Thus, we express the base ten number 132 as 246 in base 7, or as 246_7 , the little 7 indicating the base. For small numbers, with a couple of minutes practice, conversion from base 10 (decimal) to other bases, and back again can be carried out mentally. For larger numbers, mental arithmetic will prove a little awkward. Luckily there is a handy algorithm to do the conversion automatically.

For base 10 integers, we use the decimal digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. In general, for base b , the digits will be 0, 1, 2, 3, ..., $b - 1$. So, for example, base 7 numbers use digits 0, 1, 2, 3, 4, 5, 6. Conversion from the base b expansion of a number to its decimal version is a snap: For example, the meaning of 2302_5 is $2 \cdot 5^3 + 3 \cdot 5^2 + 0 \cdot 5 + 2 = 2 \cdot 125 + 3 \cdot 25 + 2 = 327_{10}$. Of course this uses the obvious algorithm:

Algorithm 27.1. Polynomial Evaluation using exponentiation

Input: the coefficients of a polynomial $d_k, d_{k-1}, \dots, d_1, d_0$ and number b

Output: the value of the polynomial at b : $p(b) = d_k \cdot b^k + d_{k-1} \cdot b^{k-1} + \dots + d_1 \cdot b + d_0$

1: $val \leftarrow d_0$

2: **for** $i = 1$ to n **do**

3: $val = val + d_i * b ** i$

4: **output** val

5: **stop**

Depending on whether you do the exponentiation by repeated multiplication, or by divide-and-conquer this algorithm will be $\mathcal{O}(k^2)$ or $\mathcal{O}(k \lg k)$.

A more efficient algorithm starts at the front end of the polynomial instead of the back end. The algorithm is called Horner's Method. One can easily verify that Horner's method is $\mathcal{O}(k)$. In fact, this is as efficient as possible.

Algorithm 27.2. Polynomial Evaluation via Horner's Method

Input: the coefficients of a polynomial $d_k, d_{k-1}, \dots, d_1, d_0$ and number b **Output:** the value of the polynomial at b : $p(b) = d_k \cdot b^k + d_{k-1} \cdot b^{k-1} + \dots + d_1 \cdot b + d_0$ 1: $val \leftarrow d_k$ 2: **for** $i = 1$ to n **do**3: $val = b * val + d_{k-i}$ 4: **output** val 5: **stop**

Ignoring the loop counter steps, the steps used by Horner's Method to evaluate 2302_5 are

- $val \leftarrow 2$
- $val \leftarrow 5 * 2 + 3 = 13$
- $val \leftarrow 5 \cdot 13 + 0 = 65$
- $val \leftarrow 5 \cdot 65 + 2 = 327$

For base conversions from base b to base 10 all the coefficients of our polynomials are in the set $\{0, \dots, b-1\}$. Horner's Method can also be used for more general polynomials. In addition, we can reverse Horner's Method to describe how to convert an integer from base 10 to base b .

Let's say the base b expansion of the integer n is $d_k d_{k-1} \dots d_2 d_1 d_0$, with the base b digits between 0 and $b-1$. That means

$$n = d_k \cdot b^k + d_{k-1} \cdot b^{k-1} + \dots + d_2 \cdot b^2 + d_1 \cdot b + d_0$$

Now, if we divide n by b , we can see the equation above tells us

$$n = (d_k \cdot b^{k-1} + d_{k-1} \cdot b^{k-2} + \dots + d_2 \cdot b + d_1)b + d_0.$$

So, the quotient is $q = d_k \cdot b^{k-1} + d_{k-1} \cdot b^{k-2} + \dots + d_2 \cdot b + d_1$, and the remainder is the base b digit d_0 of n . So, we have found the units digit in the base b expansion of n . If we repeat that process on the quotient q , the result is

$$q = (d_k \cdot b^{k-2} + d_{k-1} \cdot b^{k-3} + \dots + d_2)b + d_1$$

So, the next base b digit, d_1 appears as the remainder. Continuing in this fashion, the base b expansion is produced one digit at a time.

Briefly, to convert a positive decimal integer n to its base b representation, divide n by b , to find the quotient and the remainder. That remainder will be needed units digit. Then divide the quotient by b again, to get a new quotient and a new remainder. That remainder gives the next base b digit. Then divide the new quotient by b again, and so on. In this way producing the base b digits one after the other.

Example 27.1. To convert 14567 from decimal to base 5, the steps are:

$$14567 = 2913 \cdot 5 + 2$$

$$2913 = 582 \cdot 5 + 3$$

$$582 = 116 \cdot 5 + 2$$

$$116 = 23 \cdot 5 + 1$$

$$23 = 4 \cdot 5 + 3$$

$$4 = 0 \cdot 5 + 4.$$

So, we see that $14567 = 431232_5$. Notice that we have to give the digits in the reverse order that they were computed.

Particularly important in computer science applications of discrete mathematics are the bases 2 (called binary), 8 (called octal) and 16 (called hexadecimal, or simply hex). Thus, the decimal number 75 would be 1001011_2 (binary), 113_8 (octal) and $4B_{16}$ in hex. Note that for hex numbers, symbols will be needed to represent hex digits for 10, 11, 12, 13, 14 and 15. The letters A, B, C, D, E and F are traditionally used for these digits.

We can convert between two integer bases, neither of which is 10.

Example 27.2. Convert $n = 3355_7$ to base 5.

The least confusing way to do such a problem would be to convert n from base 7 to base 10, and then convert the base 10 expression for n to base 5. This method allows us to do all our work in base 10 where we are comfortable. In this example $n = 3 \cdot 7^3 + 3 \cdot 7^2 + 5 \cdot 7 + 5 = 1216_{10}$ which is followed by

$$1216 = 243 \cdot 5 + 1$$

$$243 = 48 \cdot 5 + 3$$

$$48 = 9 \cdot 5 + 3$$

$$9 = 1 \cdot 5 + 4$$

$$1 = 0 \cdot 5 + 1$$

So $3355_7 = 14331_5$.

An alternative method, not for the faint of heart, is convert directly from base 7 to base 5 skipping the middle-man base 10. In this method, we simply divide n by 5, take the remainder, getting the units digit, then divide the quotient by 5 to get the next digit, and so on, just as described above. The rub is that the arithmetic must all be done in base 7 and we don't know the base 7 times table very well. For example, in base 7, $3 \cdot 5 = 21_7$ is correct since three 5s add up to two 7s plus one.

The computations for the previous example would now look like

$$3355_7 = 465_7 \cdot 5_7 + 1_7 \text{ (yes, that's really correct!),}$$

$$465_7 = 66_7 \cdot 5_7 + 3_7$$

$$66_7 = 12_7 \cdot 5_7 + 3_7$$

$$12_7 = 1_7 \cdot 5_7 + 4_7$$

$$1_7 = 0_7 \cdot 5_7 + 1_7.$$

Hence, once again, we have $3355_7 = 14331_5$.

Exercises

Exercise 27.1. Convert to decimal: 21_3 , 321_4 , 4321_5 , and FED_{16} .

Exercise 27.2. Convert the decimal integer 11714 to bases 2, 6, and 16. Remember to use A to F to represent base 16 digits from 10 to 15, if needed.

Exercise 27.3. Complete the following base 7 multiplication table.

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4				
3			12			
4				22		
5						
6						

Exercise 27.4. Make base 6 addition and multiplication tables similar to the base 7 multiplication table of exercise [27.3](#).

Exercise 27.5. (For those with a sweet tooth for punishment!) Use the Euclidean algorithm to compute $\gcd(5122_7, 1312_7)$ without converting the numbers to base 10.

Problems

Problem 27.1. Convert to decimal: 12_3 , 123_4 , 1234_5 , and DDD_{16} .

Problem 27.2. Convert the decimal integer 3177 to bases 2, 6, and 16. Use A to F to represent base 16 digits from 10 to 15 as needed.

Problem 27.3. Make base 8 addition and multiplication tables like the base 7 multiplication table of exercise [27.3](#).

Problem 27.4. Using the table in problem [27.3](#), add $126_8 + 457_8$.

Problem 27.5. Using the table in problem [27.3](#), multiply $126_8 \cdot 457_8$.

PART V: Counting and Recurrences

Chapter 28: The Fundamental Counting Principles

The next few chapters will deal with the topic of **combinatorics**: the art of counting. By counting we mean determining the number of different ways of arranging objects in certain patterns or the number of ways of carrying out a sequence of tasks. For example, suppose we want to count the number of ways of making a bit string of length two. Such a problem is small enough that the possible arrangements can be counted by *brute force*. In other words, we can simply make a list of all the possibilities: 00, 01, 10, 11. So the answer is four. If the problem were to determine the number of bit strings of length fifty, the brute force method loses a lot of its appeal. For problems where brute force counting is not a reasonable alternative, there are a few principles we can apply to aid in the counting. In fact, there are just two basic principles on which all counting ultimately rests.

Throughout this chapter, all sets mentioned will be finite sets, and if A is a set, $|A|$ will denote the number of elements in A .

The **Addition Principle** says that if the sets A and B are disjoint ($A \cap B = \emptyset$), then

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

Example 28.1. If $A = \{a, b, c\}$ and $B = \{j, k, l, m, n\}$, then $|A| = 3$, $|B| = 5$, and, sure enough,

$$|A \cup B| = |\{a, b, c, j, k, l, m, n\}| = 8 = 3 + 5.$$

A different principle must be used when the sets are not disjoint. Suppose that $A = \{a, b, c\}$ and $B = \{b, c, d\}$, then $|A \cup B| = |A| + |B| - |A \cap B| = 3 + 3 - 2 = 4$ and not 6. This and its generalization are the subjects of a future section. This principle is called **inclusion-exclusion**.

Example 28.2. As another example of the addition principle, if we have a collection of 3 dogs and 5 cats, then we can select one of the animals in 8 ways since no cat is also a dog.

The addition principle is often expressed in different language: If we can do task 1 in m ways and task 2 in n ways, and the tasks are *independent* (meaning that both tasks cannot be done at the same time), then there are $m + n$ ways to do one of the two tasks. The independence of the tasks is the analog of the disjointness of the sets in the set version of the addition principle.

Yet another version of the story is if we can do a task by method 1 in m ways or by a different method in n ways, then there are $m + n$ ways to complete the task using one of the two methods.

A serious type of error is trying to use the addition principle for tasks that are not independent. For instance, suppose we want to know “In how many different ways we can select either a deuce or a six from an ordinary deck of 52 cards?”. We could let the first task be the process of selecting a deuce from the deck. That task can be done in 4 ways since there are 4 deuces in the deck. For the second task, we will take the operation of selecting a six from the deck. Again, there are 4 ways to accomplish that task. Now these tasks are independent since we cannot simultaneously pick a deuce and a six from the deck. So, according to the addition principle,

there are $4 + 4 = 8$ ways of selecting one card from a deck and having that card be either a deuce or a six.

Now consider the similar sounding question “*In how many ways can we select either a deuce or a diamond from a deck of 52 cards?*”. We could let the first task again be the operation of selecting a deuce from the deck, with 4 ways to carry out that task. And we could let the second task be the operation of selecting a diamond from the deck, with 13 ways to accomplish that. But in this case, the answer to the question is not $4 + 13 = 17$, since these tasks are not independent. It is possible to select a card that is both a deuce and a diamond. So, the addition principle cannot be used. To get the correct answer there are 13 diamonds, and there are 3 deuces besides the deuce of diamonds, and so there are actually 16 cards in the deck that are either a deuce or a diamond. That means there are 16 ways to select a card from a deck and have it turn out to be either a deuce or a diamond.

The addition principle can be extended to the case of more than two sets (or tasks, or methods): If a collection $A_1, A_2, \dots, A_n$ of sets are *pairwise disjoint* ($A_i \cap A_j = \emptyset$, whenever $i \neq j$), then

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

In terms of independent tasks: If task 1 can be completed in k_1 ways and task 2 can be completed in k_2 ways and so on until task n can be completed in k_n ways, then the total number of ways to complete the tasks is $k_1 + k_2 + \dots + k_n$. N.B. the tasks must be pairwise independent.

Example 28.3. *If we own three cars, two bikes, a motorcycle, four pairs of roller skates, and two scooters, then we can select one mode of transportation in $3 + 2 + 1 + 4 + 2 = 12$ ways.*

The addition principle is related to the logical connective *xor*. That is reasonable since the addition principle counts the number of elements in the set $A \cup B = \{x | x \in A \text{ or } x \in B\}$. In terms of tasks, the addition principle counts the number of ways to do either task 1 or task 2. When the word *or* occurs in a counting problem and we have disjointness (independence), then the addition principle is the tool to use.

The logical connective *and* is related to the second fundamental counting principle: the **multiplication principle**. The multiplication principle says:

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

An explanation of this is that $A \times B$ consists of all ordered pairs (a, b) where $a \in A$ and $b \in B$. There are $|A|$ choices for a and then $|B|$ choices for b .

In terms of tasks, the multiplication principle says that if task 1 can be done in m ways and task 2 can be done in n ways after task 1 has been done, then there are mn ways to do both tasks, the first and then the second. Here the relation with the logical connective *and* is also obvious. We need to do task 1 and task 2. Generally speaking, the appearance of *and* in a counting problem suggests the multiplication principle will come into play.

As with the addition principle, the multiplication principle can be used for situations with more than two sets or more than two tasks. For sets the multiplication principle reads

$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$. In terms of tasks, it reads, if task 1 can be done in k_1 ways, and for each of those ways, task 2 can be done in k_2 ways, and for each of those ways, task 3 can be done in k_3 ways, and so on, until for each of those ways, task n can be done in k_n ways, then we can do task 1 followed by task 2 followed by task 3, etc, followed by task n in $k_1 \cdot k_2 \cdot \dots \cdot k_n$ ways.

Example 28.4. *How many bit strings are there of length five?*

Solution. *We can think of task 1 as filling in the first (right hand) position, task 2 as filling in the second position, and so on. We can argue that we have two ways to do task 1, and then two ways to do task 2, and then two ways to do task 3, and then two ways to do task 4, and then two ways to do task 5. So, by the multiplication principle, there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$ ways to do all five tasks, and so there are 32 bit strings of length five.*

The same reasoning shows that, in general, there are 2^n bit strings of length n , when $n \geq 0$.

Example 28.5. *Suppose we are buying a car with five choices for the exterior color and three choices for the interior color. Then there is a total of $3 \cdot 5 = 15$ possible color combinations that we can choose from. The first task is to select an exterior color, and there are 5 ways to do that. The second task is to select an interior color, and there are 3 ways to do that. So the multiplication principle says there are 15 ways total to do both tasks. Notice that there is no requirement of independence of tasks when using the multiplication principle. Also notice that the number of ways of doing the second task **must** be the same no matter what choice is made for doing the first task.*

Example 28.6. *For another, slightly more complicated, example of the multiplication principle in action, suppose we wanted to make a two-digit number using the digits 1, 2, 3, 4, 5, 6, 7, 8, and 9. How many different two-digit numbers could we form? Let's make the first task filling in the left digit, and the second task filling in the right digit. There are 9 ways to do the first task. And, no matter how we do the first task, there are 9 ways to do the second task as well. So, by the multiplication principle, there are $9 \cdot 9 = 81$ possible two-digit numbers.*

Example 28.7. *Now, let's change the problem in example [28.6](#) a little bit. Suppose we wanted two-digit numbers made up of those same nine digits, but we do not want to use a digit more than once in any of the numbers. In other words, 37 and 91 are OK, but we do not want to count 44 as a possibility. We can still make the first task filling in the left digit, and the second task filling in the right digit. And, as before, there are 9 ways to do the first task. But now, once the first task has been done, there are only 8 ways to do the second task, since the digit used in the first task is no longer available for doing the second task. For instance, if the digit 3 was selected in the first task, then for the second task, we will have to choose from the eight digits 1, 2, 4, 5, 6, 7, 8, and 9. So, according to the multiplication principle, there are $9 \cdot 8 = 72$ such numbers.*

No matter how the first task was done, there are always 8 ways to do the second task in sequence. What if you chose to pick the second digit first?

Example 28.8. *Just for fun, here is another way to see the answer in example 28.7 is 72. We saw above that there are 81 ways to make a two-digit number when we allow repeated digits. But there are 9 two-digit numbers that do have repeated digits (namely 11, 22, ..., 99). That means there must be $81 - 9 = 72$ two-digit numbers without repeated digits.*

The trick we used in example 28.8 looks like a new counting principle, but it is really the addition principle in disguise. Here's the idea. Call the set of all the two-digit numbers (not using 0) T , call the set with no repeated digits N , and call the set with repeated digits R . By the addition principle, $|T| = |N| + |R|$, so $|N| = |T| - |R|$. This is a very common trick which we may call the **exclusion principle**.

Generally, suppose we are interested in counting some arrangements, let's call them the *Good* arrangements. But it is not easy for some reason to count the *Good* arrangements directly. So, instead, we count the *Total* number of arrangements and subtract the number of *Bad* arrangements: $Good = Total - Bad$.

Let's have another example of this trick.

Example 28.9. *By a word of length five, we will mean any string of five letters from the 26-letter alphabet. How many words contain at least one vowel. The vowels are: a, e, i, o, u. By the multiplication principle, there is a total of 26^5 possible words of length five. The bad words are made up of only the 21 non-vowels. So, by the exclusion principle the number of good words is $26^5 - 21^5$.*

As in example 28.9, most interesting counting problems involve a combination of both the addition and multiplication principles.

Example 28.10. *Suppose we wanted to count the number of different possible bit strings of length five that start with either three 0's or with two 1's. Recall that a bit string is a list of 0's and 1's, and the length of the bit string is the total number of 0's and 1's in the list. So, here are some bit strings that satisfy the stated conditions: 00001, 11111, 11011, and 00010. On the other hand, the bit strings 00110 and 10101 do not satisfy the required condition.*

To complete this problem, let's first count the number of good bit strings that start with three 0's. In this case, we can think of the construction of such a bit string as doing five tasks, one after the other, filling in the leftmost bit, then the next one, then the third, the next, and finally the last bit. There is only one way to do the first three tasks, since we need to fill in 0's in the first three positions. But there are two ways to do the last two tasks, and so, according to the multiplication principle there are $1 \cdot 1 \cdot 1 \cdot 2 \cdot 2 = 4$ bit strings of length five starting with three 0's. Using the same reasoning, there are $1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 = 8$ bit strings of length five starting with two 1's. Now, a bit string cannot start with both three 0's and also with two 1's, (in other words, starting with three 0's and starting with two 1's are independent). And so, according to the addition principle, there will be a total of $4 + 8 = 12$ bit strings of length five starting with either three 0's or two 1's.

Example 28.11. *How many words of six letters (repeats OK) contain exactly one vowel?*

Solution. *Let's break the construction of a good word down into a number of sequential tasks.*

- *Task 1: Select a spot for the vowel: 6 choices.*
- *Task 2: Select a vowel for that spot: 5 choices.*
- *Task 3: Fill the first empty spot with a non-vowel: 21 choices.*
- *Task 4: Fill the next empty spot with a non-vowel: 21 choices.*
- *Task 5: Fill the next empty spot with a non-vowel: 21 choices.*
- *Task 6: Fill the next empty spot with a non-vowel: 21 choices.*
- *Task 7: Fill the last empty spot with a non-vowel: 21 choices.*

By the multiplication principle the number of good words is $6 \cdot 5 \cdot 21^5$.

Example 28.12. *Count the number of strings on license plates which either consist of three capital English letters followed by three digits or consist of two digits followed by four capital English letters.*

Solution. *Let A be the set of strings which consist of three capital English letters followed by three digits and B be the set of strings which consist of two digits followed by four capital English letters. By the multiplication principle $|A| = 26^3 \cdot 10^3$ since there are 26 capital English letters and 10 digits. Also, by the multiplication principle $|B| = 10^2 \cdot 26^4$. Moreover we have that $A \cap B = \emptyset$, by the addition principle the answer is $26^3 \cdot 10^3 + 10^2 \cdot 26^4$.*

In the previous examples we might continue on with the arithmetic. For instance, in the last, example 28.12, using the distributive law on our answer to factor out common terms we see that $|A \cup B| = 10^2 \cdot 26^3(10 + 26)$ is an equivalent answer. Thus $|A \cup B| = 10^2 \cdot 26^3 \cdot 36$ and that gives $|A \cup B| = 100 \cdot 17576 \cdot 36 = 63,273,600$.

Of all of these answers the most valuable is probably $26^3 \cdot 10^3 + 10^2 \cdot 26^4$, since **the form of the answer is indicative of the manner of solution**. We can readily observe that the addition principle was applied to two disjoint subcases. For each subcase the multiplication principle was applied to compute the intermediate answer. As a general rule answers to counting problems should be left in this un-computed form.

Exercises

Exercise 28.1. *To meet the science requirement a student must take one of the following courses: a choice of 5 biology courses, 4 physics courses, or 6 chemistry courses. In how many ways can one course be selected?*

Exercise 28.2. *Using the data of problem 1, a student has decided to take one biology, one physics, and one chemistry course. How many different such selections are possible?*

Exercise 28.3. *A serial code is formed in one of three ways: (1) two letters followed by two digits, or (2) three letters followed by one digit, or (3) four letters. How many different codes are there? (Unless otherwise indicated, letters will mean upper case letters chosen from the usual 26-letter alphabet and digits are selected from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.)*

Exercise 28.4. *How many words of length six are there if letters may be repeated? (Examples: BBBXBB, ABATBC are OK).*

Exercise 28.5. *How many words of length six are there if letters may not be repeated? (Examples: BBBBXB, ABATJC are bad but ABXHYP is OK).*

Exercise 28.6. *A true/false test contains 25 questions.*

- a) *How many ways can a student complete the test if every question must be answered?*
- b) *How many ways can a student complete the test if questions can be left unanswered?*

Exercise 28.7. *How many binary strings of length less than or equal to nine are there?*

Exercise 28.8. *How many eight-letter words contain at least one A?*

Exercise 28.9. *How many seven-letter words contain at most one A?*

Exercise 28.10. *How many nine-letter words contain at least two A's?*

Problems

Problem 28.1. *My piggy bank contains 20 pennies, 4 nickels, 7 dimes, and 2 quarters. In how many ways can I select one coin?*

Problem 28.2. *My piggy bank contains 20 pennies, 4 nickels, 7 dimes, and 2 quarters. In how many ways can I select four coins, one of each value?*

Problem 28.3. *A multiple-choice test contains 10 questions. There are four possible answers for each question.*

a) *How many ways can a student complete the test if every question must be answered?*

b) *How many ways can a student complete the test if questions can be left unanswered?*

Problem 28.4. *Computer ID's are length seven strings made up of any combination of seven different letters and digits. How many different ID's are there?*

Problem 28.5. *Computer ID's are length seven strings made up of any combination of seven letters and digits, with repeats allowed. How many different ID's are there?*

Problem 28.6. *A code word is either a sequence of three letters followed by two digits or two letters followed by three digits. (Unless otherwise indicated, letters will mean upper case letters chosen from the usual 26-letter alphabet and digits are selected from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.) How many different code words are possible?*

Problem 28.7. *Code words consist of five letters followed by five digits. How many code words contain at least one X?*

Problem 28.8. *Code words consist of five letters followed by five digits. How many code words contain exactly one X?*

Problem 28.9. *Code words consist of five letters followed by five digits. How many code words contain exactly two X's?*

Problem 28.10. *How many bit strings of length ten begin and end with 1's?*

Problem 28.11. *How many bit strings of length at least two but no more than ten begin and end with 1's?*

Chapter 29: Permutations and Combinations

By a **permutation** of a set of objects we mean a listing of the objects of the set in a specific order. For example, there are six possible permutations of the set $A = \{a, b, c\}$. They are

$$abc, acb, bac, bca, cab, cba.$$

The multiplication principle explains why there are six permutations of A : there are 3 choices for the first letter, once that choice has been made there are 2 choices for the second letter, and that leaves only 1 choice for the last letter. So, the total number of permutations is $3 \cdot 2 \cdot 1 = 6$.

A set with n elements is called an **n –set**. We have just shown that a 3 –set has 6 permutations. The same reasoning shows that an n –set has $n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 2 \cdot 1 = n!$ permutations. The total number of different ways to arrange a deck of cards is $52!$, a number with 68 digits:

$$80658175170943878571660636856403766975289505440883277824000000000000.$$

Instead of forming a permutation of all the elements of an n –set, we might consider the problem of first selecting some of the elements of the set, say r of them, and then forming a permutation of just those r elements. In that case we say we have formed an **r –permutation** of the n –set. All the possible 2 –permutations of the 4 –set $A = \{a, b, c, d\}$ are

$$ab, ac, ad, ba, bc, bd, ca, cb, cd, da, db, dc.$$

Hence, there are twelve 2 –permutations of a 4 –set.

Notation. In general, $P(n, r)$ denotes the number of different r –permutations of an n –set.

As above the number of 2 –permutations of a 4 –set is $P(4, 2) = 12$.

The multiplication principle provides a simple formula for $P(n, r)$. There are n choices for the first element, and once that choice has been made, there are $n - 1$ choices for the second element, then $n - 2$ for the third, and so on, until finally, there are $n - (r - 1) = n - r + 1$ choices for the r th element. So $P(n, r) = n(n - 1) \cdot \dots \cdot (n - r + 1)$. That expression can be written more neatly as follows:

$$\begin{aligned} P(n, r) &= n(n - 1) \cdot \dots \cdot (n - r + 1) \\ &= \frac{n(n - 1) \cdot \dots \cdot (n - r + 1)(n - r)(n - r - 1) \dots \cdot 2 \cdot 1}{(n - r)(n - r - 1) \dots \cdot 2 \cdot 1} = \frac{n!}{(n - r)!} \end{aligned}$$

Example 29.1. The number of ways of selecting a president, vice-president, secretary, and treasurer from a group of 20 people is $P(20, 4)$ (assuming no person can hold more than one office). If you want the actual numerical value, it is $\frac{20!}{(20-4)!} = 20 \cdot 19 \cdot 18 \cdot 17 = 116280$. But the best way to write the answer is $P(20, 4)$ or $20!/16!$.

Example 29.2. *How many one-to-one functions are there from a 5 –set to a 7 –set?*

While this question doesn't sound on the surface like a problem of permutations, it really is. Suppose the 5 –set is $A = \{1, 2, 3, 4, 5\}$ and the 7 –set is $B = \{a, b, c, d, e, f, g\}$. One example of a one-to-one function from A to B would be $f(1) = a, f(2) = c, f(3) = g, f(4) = b, f(5) = d$. But, if we agree to think of the elements of A listed in their natural order, we could specify that function more briefly as $acgbd$. In other words, each one-to-one function specifies a 5 –permutation of B , and, conversely, each 5 –permutation of B specifies a one-to-one function. So, the number of one-to-one functions from a 5 –set to a 7 –set is equal to the number of 5 –permutations of a 7 –set, and that is $P(7, 5) = 2520$.

The same reasoning shows there are $P(n, r)$ one-to-one functions from an r –set to an n –set.

Example 29.3. *Here are a few easily seen values of $P(n, r)$:*

- (1) $P(n, n) = n!$
- (2) $P(n, 1) = n$
- (3) $P(n, 0) = 1$
- (4) $P(n, r) = 0$ if $r > n$.

When forming permutations, the order in which the elements are listed is important. But there are many cases when we are interested only in which elements are selected and we do not care about the order. For example, when playing poker, a hand consists of five cards dealt from a standard 52 –card deck. The order in which the cards arrive in a hand does not matter, only the final selection of the five cards is important. When order is not important, the selection is called a combination rather than a permutation. More carefully, an **r –combination** from an n –set is an r –subset of the n –set. In other words, an r –combination of an n –set is an unordered selection of r distinct elements from the n –set.

Example 29.4. *The 2 –combinations of the 5 –set $\{a, b, c, d, e\}$ are*

$$\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}, \{d, e\}.$$

Notation. *The number of r –combinations from an n –set is denoted $C(n, r)$ or $\binom{n}{r}$.*

Example 29.5. *Here are a few easily seen values of $C(n, r)$:*

- (1) $C(n, n) = 1$
- (2) $C(n, 1) = n$
- (3) $C(n, 0) = 1$; the only set with 0 elements is $\emptyset$.
- (4) $C(n, r) = 0$ if $r > n$ since a subset cannot contain more objects than its superset.

There is a compact formula for $C(n, r)$ which can be derived using the multiplication principle in a sort of back-handed way. An r –permutation of an n –set can be built using a sequence of two

tasks. First, select r elements of the n -set. There are $C(n, r)$ ways to do that task. Next, arrange those r elements in some specific order. There are $r!$ ways to do that task. So, according to the multiplication principle, the number of r –permutations of an n –set will be $C(n, r)r!$.

However, we know that the number of r –permutations of an n –set is $P(n, r)$. So, we conclude that $P(n, r) = C(n, r)r!$, or, rearranging that, we see

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

Example 29.6. *Suppose we have a club with 20 members. If we want to select a committee of 4 members, then there are*

$$C(20, 4) = \frac{20!}{4!16!} = \frac{20 \cdot 19 \cdot 18 \cdot 17}{4 \cdot 3 \cdot 2 \cdot 1} = 4845$$

ways to do this since the order of people on the committee doesn't matter.

Compare this answer with example [29.1](#) where we counted the number of possible selections for president, vice-president, secretary, and treasurer from the group of 20. The difference between the two cases is that the earlier example is a question about permutations (order matters), whereas this example is a question about combinations (order does not matter).

Exercises

Exercise 29.1. *In how many ways can the 26 volumes (labeled A through Z) of the Encyclopedia of Pseudo-Science be placed on a shelf?*

Exercise 29.2. *In how many ways can those same 26 volumes be placed on a shelf if superstitions demand the volumes labeled with vowels must be adjacent? In how many ways can they be placed on the shelf obeying the conflicting superstition that volumes labeled with vowels cannot touch each other?*

Exercise 29.3. *For those same 26 volumes, how many ways can they be placed in a two-shelf bookcase if volumes A-M go on the top shelf and N -Z go on the bottom shelf?*

Exercise 29.4. *In how many ways can seven men and four women sit in a row if the men must sit together?*

Exercise 29.5. *20 players are to be divided into two 10 –person teams. In how many ways can that be done?*

Exercise 29.6. *A lottery ticket consists of five different integers selected from 1 to 99. How many different lottery tickets are possible? How many tickets would you need to buy to have a one-in-a-million chance of winning by matching all five randomly selected numbers?*

Exercise 29.7. *A committee of size six is selected from a group of nine deans and thirteen professors.*

- (a) *How many different committees are possible?*
- (b) *How many committees are possible if there must be exactly two deans on the committee?*
- (c) *How many committees are possible if professors must outnumber deans on the committee?*

Problems

Problem 29.1. *In how many ways can the ten digits be written in a row?*

Problem 29.2. *In how many ways can the ten digits be written in a row if the odd digits have to be adjacent?*

Problem 29.3. *In how many ways can the ten digits be written in a row if the even and odd digits have to alternate?*

Problem 29.4. *How many bit strings of length ten have exactly four 0's?*

Problem 29.5. *How many bit strings of length ten have at most four 0's?*

Problem 29.6. *How many length twenty strings of a's, b's, and c's have ten a's, six b's, and four c's?*

Problem 29.7. *How many bit strings of length ten have more 0's than 1's?*

Problem 29.8. *In how many ways can a subset of two numbers from 1 to 100 (inclusive) be selected if the selected numbers cannot be consecutive?*

Chapter 30: The Binomial Theorem and Pascal's Triangle

The quantity $C(n, k)$ is also written $\binom{n}{k}$ and called a *binomial coefficient*. It gives the number of k –subsets of an n –set, or, equivalently, it gives the number of ways of selecting k distinct items from n items.

Facts about the binomial coefficients can be proved by the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ using algebra. But often the same facts can be proved much more neatly by recognizing $\binom{n}{k}$ gives the number of k –subsets of an n –set. This second sort of proof is called a combinatorial proof. Here is an example of each type of proof.

Theorem 30.1 (Pascal's Identity). *Let n and k be non-negative integers, then*

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

Proof. (a combinatorial proof) Let S be a set with $n + 1$ elements. Select one particular element $a \in S$. There are two ways to produce a subset of S of size k . We can include a in the subset and toss in $k - 1$ of the remaining elements of S . There are $\binom{n}{k-1}$ ways to do that. Or we can avoid a and choose all k elements from the other n elements of S . There are $\binom{n}{k}$ ways to do that. So, by the addition principle there are a total of $\binom{n}{k-1} + \binom{n}{k}$ subsets of size k of S . But we know that there are $\binom{n+1}{k}$ subsets of S of size k so we conclude that $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$. ■

Proof. (an algebraic proof)

$$\begin{aligned} \binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{1}{n-k+1} + \frac{1}{k} \right) \\ &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{k}{k(n-k+1)} + \frac{n-k+1}{k(n-k+1)} \right) \\ &= \frac{n!}{(k-1)!(n-k)!} \frac{k + (n-k) + 1}{k(n-k+1)} \\ &= \frac{n!}{(k-1)!(n-k)!} \frac{n+1}{k(n-k+1)} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \binom{n+1}{k}. \quad \blacksquare \end{aligned}$$

The idea of a combinatorial proof is to ask a counting problem that can be answered in two different ways and then conclude the two answers must be equal. In the proof above, we asked how many k –subsets there are of an $(n + 1)$ –set. We provided an argument to show two answers were correct: $\binom{n+1}{k}$ and $\binom{n}{k-1} + \binom{n}{k}$. So, we concluded the two answers must be equal:

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

As in the combinatorial proof of Pascal's Identity [30.1](#), such arguments can be much less work, far less tedious, and much more illuminating, than algebraic proofs. Unfortunately, they can also be much more difficult to discover since it is necessary to dream up a good counting problem that will have as answers the two expressions we are trying to show are equal, and there is no algorithm for coming up with such a suitable counting problem.

Example 30.2. Give a combinatorial proof of $\binom{n}{k} = \binom{n}{n-k}$.

Solution. To provide a combinatorial proof, we ask how many ways are there to grab k elements of an n –set? One answer is of course $\binom{n}{k}$. But a second way to view the problem is to select the k items by deciding which $n - k$ items not to pick. Since there are $\binom{n}{n-k}$ ways to select $n - k$ items not to pick, there must be $\binom{n}{n-k}$ ways to select k elements from an n –set. Since the two answers must be equal we conclude that $\binom{n}{k} = \binom{n}{n-k}$. ■

Example 30.3. Give a combinatorial proof of *Vandermonde's Identity*:

Solution. Consider the set $\{a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m\}$ of $n + m$ elements. We ask how many k –subsets does the set have?

One answer is of course $\binom{n+m}{k}$.

Another answer runs

We can select 0 of the a_i 's and k of the b_j 's: There are $\binom{n}{0}\binom{m}{k}$ ways to do that.

Or we can select 1 of the a_i 's and $k - 1$ of the b_j 's: There are $\binom{n}{1}\binom{m}{k-1}$ ways to do that.

Or we can select 2 of the a_i 's and $k - 2$ of the b_j 's: There are $\binom{n}{2}\binom{m}{k-2}$ ways to do that.

And so on, until we reach the option of selecting k of the a_i 's and 0 of the b_j 's: There are $\binom{n}{k}\binom{m}{0}$ ways to do that.

By the addition principle the total is

$$\binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \binom{n}{2}\binom{m}{k-2} + \dots + \binom{n}{k}\binom{m}{0}. \quad \blacksquare$$

Row 0:				$\binom{0}{0}$			
Row 1:			$\binom{1}{0}$		$\binom{1}{1}$		
Row 2:		$\binom{2}{0}$		$\binom{2}{1}$		$\binom{2}{2}$	
Row 3:	$\binom{3}{0}$		$\binom{3}{1}$		$\binom{3}{2}$		$\binom{3}{3}$
Row 4:	$\binom{4}{0}$	$\binom{4}{1}$		$\binom{4}{2}$		$\binom{4}{3}$	$\binom{4}{4}$
Row 5:	$\binom{5}{0}$	$\binom{5}{1}$	$\binom{5}{2}$	$\binom{5}{3}$	$\binom{5}{4}$	$\binom{5}{5}$	

Figure 30.1: Pascal's Triangle

The binomial coefficients are so named because they appear when a binomial $x + y$ is raised to an integer power $k \geq 0$. To appreciate the connection, let's look at a table of the binomial coefficients $\binom{n}{k}$. The table is arranged in rows starting with row $n = 0$, and within each row, the entries are arranged from left to right for $k = 0, 1, 2, \dots, n$. The result, called Pascal's Triangle, is shown in figure [30.1](#).

Filling in the numerical values for the binomial coefficients gives the table shown in figure [30.2](#).

Row 0:						1					
Row 1:					1			1			
Row 2:				1		2			1		
Row 3:			1		3		3			1	
Row 4:		1		4		6		4		1	
Row 5:	1		5		10		10		5		1

Figure 30.2: Pascal's Triangle (numerical)

Note that we number the rows starting with 0. We already know quite a bit about the entries in Pascal's Triangle.

Since $\binom{n}{0} = \binom{n}{n} = 1$ for all n , each row begins and ends with a 1.

From the symmetry formula $\binom{n}{n} = \binom{n}{n-k}$, the rows read the same in both directions.

From Pascal's Identity, each entry in a row is the sum of the two entries diagonally above it. This last fact makes it easy to add new rows to Pascal's Triangle

The numbers in the first, second, and third rows of Pascal's triangle probably seem familiar. In fact, we see that

$$(x + y)^0 = 1$$

$$(x + y)^1 = x + y = 1 \cdot x + 1 \cdot y$$

$$(x + y)^2 = x^2 + 2xy + y^2 = 1 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = 1 \cdot x^3 + 3 \cdot x^2y + 3 \cdot xy^2 + 1 \cdot y^3$$

The coefficients in these binomial expansions are exactly the entries in the corresponding rows of Pascal's Triangle. We start at the 0^{th} row: $(x + y)^0 = 1$ because it works.

The fact that the coefficients in the expansion of the binomial $(x + y)^n$ (where $n \geq 0$ is an integer) can be read off from the n^{th} row of Pascal's Triangle is called the Binomial Theorem. We will give two proofs of this theorem, one by induction, and the other a combinatorial proof.

Theorem 30.4 (The Binomial Theorem). *When n is a non-negative integer and $x, y \in \mathbb{R}$*

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

Proof. We proceed by induction on n . When $n = 0$ the result is clear. So, suppose that for some $m \geq 0$ we have

$$(x + y)^m = \sum_{k=0}^m \binom{m}{k} x^k y^{m-k}, \text{ for any } x, y \in \mathbb{R}.$$

Then $(x + y)^{m+1} = (x + y)^m(x + y)$, by recursive definition of integral exponents.

$$= \left(\sum_{k=0}^m \binom{m}{k} x^k y^{m-k} \right) (x + y), \text{ by inductive hypothesis.}$$

$$= \left[\sum_{k=0}^m \binom{m}{k} x^{k+1} y^{m-k} \right] + \left[\sum_{k=0}^m \binom{m}{k} x^k y^{m+1-k} \right], \text{ by distribution}$$

$$\begin{aligned}
 &= \binom{m}{m} x^{m+1} + \left[\sum_{k=0}^{m-1} \binom{m}{k} x^{k+1} y^{m-k} \right] + \left[\sum_{k=1}^m \binom{m}{k} x^k y^{m+1-k} \right] + \binom{m}{0} y^{m+1} \\
 &= \binom{m}{m} x^{m+1} + \left[\sum_{l=1}^m \binom{m}{l-1} x^l y^{m-(l-1)} \right] + \left[\sum_{k=1}^m \binom{m}{k} x^k y^{m+1-k} \right] + \binom{m}{0} y^{m+1} \\
 &= \binom{m}{m} x^{m+1} + \left[\sum_{l=1}^m \binom{m}{l-1} x^l y^{m+1-l} \right] + \left[\sum_{k=1}^m \binom{m}{k} x^k y^{m+1-k} \right] + \binom{m}{0} y^{m+1} \\
 &= \binom{m}{m} x^{m+1} + \left[\sum_{k=1}^m \left\{ \binom{m}{k-1} + \binom{m}{k} \right\} x^k y^{m+1-k} \right] + \binom{m}{0} y^{m+1} \\
 &= \binom{m+1}{m+1} x^{m+1} + \left[\sum_{k=1}^m \binom{m+1}{k} x^k y^{m+1-k} \right] + \binom{m+1}{0} y^{m+1} \\
 &= \sum_{k=0}^{m+1} \binom{m+1}{k} x^k y^{m+1-k}. \blacksquare
 \end{aligned}$$

Now, let's look at a combinatorial proof of the Binomial Theorem.

Proof. When the binomial $(x + y)^n = (x + y)(x + y)(x + y) \cdots (x + y)$ is expanded, the terms are produced by selecting either the x or the y from each of the n factors $x + y$ appearing on the left-hand side of the equation. The number of ways of selecting exactly k x 's from the n available is $\binom{n}{k}$ and so that will be the coefficient of the term $x^k y^{n-k}$ in the expansion. ■

Example 30.5. The coefficient of $x^7 y^3$ in the expansion of $(x + y)^{10}$ is

$$\binom{10}{7} = \frac{10!}{3!7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120.$$

Example 30.6. The coefficient of $x^7 y^3$ in the expansion of $(2x - 3y)^{10}$ is

$$\binom{10}{7} 2^7 (-3)^3 = \frac{10!}{3!7!} 2^7 (-3)^3 = -\frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} 2^7 3^3 = -120 \cdot 128 \cdot 27 = -414720.$$

From the binomial theorem we can derive facts such as

Theorem 30.7. A finite set with n elements has 2^n subsets.

Proof. By the addition principle the number of subsets of an n -set is

$$\sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k}.$$

By the Binomial Theorem $\sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = (1 + 1)^n = 2^n$. ■

Theorem 30.8. *If $n \geq 1$, then*

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

Proof. By the Binomial Theorem

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

Exercises

Exercise 30.1. Determine the sixth row of Pascal's Triangle.

Exercise 30.2. Determine the coefficient of x^3y^7 in the expansion of $(3x - 2y)^{10}$.

Exercise 30.3. Give an algebraic proof that

$$\binom{2n}{2} = 2 \binom{n}{2} + n^2.$$

Exercise 30.4. Give an algebraic proof that

$$\binom{r}{s} \binom{s}{t} = \binom{r}{t} \binom{r-t}{s-t}.$$

Exercise 30.5. Give a combinatorial proof that

$$\binom{r}{s} \binom{s}{t} = \binom{r}{t} \binom{r-t}{s-t}.$$

Exercise 30.6. Using the same reasoning as in the combinatorial proof of the Binomial Theorem, determine the coefficient of $x^4y^5z^6$ in the expansion of $(x + y + z)^{15}$.

Exercise 30.7. Show that if p is a prime and $0 < k < p$, then p divides $\binom{p}{k}$

Hint: When $\binom{p}{k}$ is written out, how many times does p occur as a factor of the numerator and how many times as a factor of the denominator?

Problems

Problem 30.1. Determine the seventh row of Pascal's Triangle.

Problem 30.2. Determine the coefficient of x^5y^2 in the expansion of $(2x - 5y)^7$.

Problem 30.3. Give a combinatorial proof that $\binom{2n}{2} = 2\binom{n}{2} + n^2$.

Hint: How many ways are there to select a 2-subset of $\{a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n\}$?

Problem 30.4. Give an algebraic proof that

$$\binom{n}{2} \binom{n-2}{m-2} = \binom{n}{m} \binom{m}{2}.$$

Problem 30.5. Give a combinatorial proof that

$$\binom{n}{2} \binom{n-2}{m-2} = \binom{n}{m} \binom{m}{2}.$$

Problem 30.6. Give an algebraic proof that

$$\binom{n}{m} = n \binom{n-1}{m-1}.$$

Problem 30.7. Give a combinatorial proof that

$$\binom{n}{m} = n \binom{n-1}{m-1}.$$

Problem 30.8. Give a combinatorial proof that

$$\binom{3m}{3} = \binom{m}{3} + 2m \binom{m}{2} + m \binom{2m}{2} + \binom{2m}{3}.$$

Problem 30.9. Determine the coefficient of $x^3y^2z^5$ in the expansion of $(x + 2y - 3z)^8$.

Chapter 31: Inclusion/Exclusion Counting

As we saw in Chapter 28 the addition principle will not correctly compute the number $|A \cup B|$ when A and B are not disjoint. We posited that the correct formula would be

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

This is the basic principle of **Inclusion/Exclusion**. We can validate this basic formula by first noticing that $A \cup B = (A - B) \cup B$ where $(A - B) \cap B = \emptyset$. So that

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

by the addition principle.

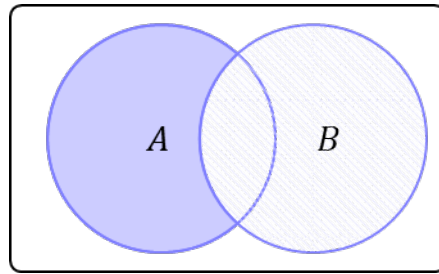


Figure 31.1: $A \cup B = (A - B) \cup B$

Next we use the fact that A is the disjoint union of $(A - B)$ and $A \cap B$. Therefore, we have that $|A| = |A - B| + |A \cap B|$ also known as $|A - B| = |A| - |A \cap B|$.

By substitution we get $|A \cup B| = |A - B| + |B| = |A| - |A \cap B| + |B|$. And finally rearrange to obtain

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

Example 31.1. How many students are there in a discrete math class if 15 students are computer science majors, 7 are math majors, and 3 are double majors in math and computer science?

Solution. Let C denote the subset of computer science majors in the class, and M denote the math majors. Then $|C| = 15$, $|M| = 7$ and $|C \cap M| = 3$. So by the principle of inclusion/exclusion there are $|C| + |M| - |C \cap M| = 15 + 7 - 3 = 19$ students in the class. $\square$

Example 31.2. How many integers between 1 and 1000 are divisible by either 7 or 11?

Solution. Let S denote the set of integers between 1 and 1000 divisible by 7, and E denote the set of integers between 1 and 1000 divisible by 11. We count the number of integers in $S \cup E$. By the principle of inclusion/exclusion, we have

$$\begin{aligned} |S \cup E| &= |S| + |E| - |S \cap E| = \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{11} \right\rfloor - \left\lfloor \frac{1000}{77} \right\rfloor \\ &= 142 + 90 - 12 = 220. \end{aligned}$$

This argument justifying the principle of inclusion/exclusion does not generalize nicely to the case where we have sets $A_1, \dots, A_n$. So, we turn to the Binomial Theorem and combinatorial argument.

Theorem 31.3. (Inclusion/Exclusion) *Given finite sets $A_1, A_2, \dots, A_n$*

$$\left| \bigcup_{i=1}^n A_i \right| = \left[\sum_{i=1}^n |A_i| \right] - \left[\sum_{1 \leq i < j \leq n} |A_i \cap A_j| \right] + \left[\sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \right] + \dots + (-1)^{n-1} \left| \bigcap_{i=1}^n A_i \right|.$$

Proof. This is a corollary of the Theorem 31.4. ■

Theorem 31.4. *Given finite sets $A_1, A_2, \dots, A_n$*

$$\left| \bigcap_{i=1}^n \bar{A}_i \right| = |\mathcal{U}| - \left[\sum_{i=1}^n |A_i| \right] + \left[\sum_{1 \leq i < j \leq n} |A_i \cap A_j| \right] + \dots + (-1)^n \left| \bigcap_{i=1}^n A_i \right|.$$

Proof. Let $x \in \mathcal{U}$. Then two cases to consider are 1) $x \notin A_i$ for all i and 2) $x \in A_i$ for exactly p of the sets A_i , where $1 \leq p \leq n$.

In the first case, x is counted once on the left-hand side. It is also counted only once on the right-hand side in the $|\mathcal{U}|$ term. It is not counted in any of the subsequent terms on the right-hand side.

In the second case, x is not counted on the left-hand side, since it is not in the general intersection of the complements. Denote the term $|\mathcal{U}|$ as the 0th term, $\sum_{i=1}^n |A_i|$ as the 1st term, etc. Since x is a member of exactly p of the sets $A_1, \dots, A_n$, it gets counted $\binom{p}{m}$ times in the m th term. (Remember that $\binom{m}{k} = 0$, when $k > m$)

So, the total number of times x is counted on the right-hand side is

$$\binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \dots + (-1)^p \binom{p}{p}.$$

All terms of the form $\binom{p}{k}$, where $k > p$ do not contribute. By the binomial theorem

$$0 = (1 + (-1))^p = \binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \dots + (-1)^p \binom{p}{p}.$$

So, the count is correct. ■

We will rely on Theorem 31.4 version in chapter 33.

Example 31.5. *How many integers between 1 and 1000 are divisible by at least one of 7, 9, and 11?*

Solution. Let S denote the set of integers between 1 and 1000 divisible by 7, let N denote the set of integers between 1 and 1000 divisible by 9, and E denote the set of integers between 1 and 1000 divisible by 11. We need to count the number of integers in $S \cup N \cup E$. By the principle of inclusion/exclusion,

$$\begin{aligned}
 |S \cup N \cup E| &= |S| + |N| + |E| - |S \cap N| - |S \cap E| - |N \cap E| + |S \cap N \cap E| \\
 &= \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{9} \right\rfloor + \left\lfloor \frac{1000}{11} \right\rfloor - \left\lfloor \frac{1000}{63} \right\rfloor - \left\lfloor \frac{1000}{77} \right\rfloor - \left\lfloor \frac{1000}{99} \right\rfloor + \left\lfloor \frac{1000}{693} \right\rfloor \\
 &= 142 + 111 + 90 - 15 - 12 - 10 + 1 = 307.
 \end{aligned}$$

Example 31.5. How many students are in a calculus class if 14 are math majors, 22 are computer science majors, 15 are engineering majors, and 13 are chemistry majors, if 5 students are double majoring in math and computer science, 3 students are double majoring in chemistry and engineering, 10 are double majoring in computer science and engineering, 4 are double majoring in chemistry and computer science, none are double majoring in math and engineering and none are double majoring in math and chemistry, and no student has more than two majors?

Solution. Let A_1 denote the math majors, A_2 denote the computer science majors, A_3 denote the engineering majors, and A_4 the chemistry majors. Then the information given is

$$\begin{aligned}
 |A_1| &= 14, |A_2| = 22, |A_3| = 15, |A_4| = 13, \\
 |A_1 \cap A_2| &= 5, |A_1 \cap A_3| = 0, |A_1 \cap A_4| = 0, \\
 |A_2 \cap A_3| &= 10, |A_2 \cap A_4| = 4, |A_3 \cap A_4| = 3, \\
 |A_1 \cap A_2 \cap A_3| &= 0 = |A_1 \cap A_2 \cap A_4| = |A_1 \cap A_3 \cap A_4| = |A_2 \cap A_3 \cap A_4|, \\
 \text{and } |A_1 \cap A_2 \cap A_3 \cap A_4| &= 0.
 \end{aligned}$$

So, by inclusion/exclusion the number of students in the class is

$$14 + 22 + 15 + 13 - 5 - 0 - 0 - 10 - 4 - 3 + 0 + 0 + 0 + 0 - 0 = 42.$$

Example 31.6. How many ternary strings (using 0's, 1's and 2's) of length 8 either start with a 1, end with two 0's or have 4th and 5th positions 12, respectively?

Solution. Let A_1 denote the set of ternary strings of length 8 which start with a 1, A_2 denote the set of ternary strings of length 8 which end with two 0's, and A_3 denote the set of ternary strings of length 8 which have 4th and 5th positions 12. By inclusion-exclusion, the answer is

$$3^7 + 3^6 + 3^6 - 3^5 - 3^5 - 3^4 + 3^3.$$

For the form of inclusion/exclusion where we are counting the size of a union, there will always be $2^n - 1$ terms on the right-hand side of the equation in the case where we have n sets.

For the 2nd form of inclusion/exclusion where we are counting the size of the intersection of complements, there will always be 2^n terms on the right-hand side of the equation in the case where we have n sets.

Exercises

Exercise 31.1. *At a certain college no student is allowed more than two majors. How many students are in the college if there are 70 math majors, 160 chemistry majors, 230 biology majors, 56 geology majors, 24 physics majors, 35 anthropology majors, 12 double math-physics majors, 10 double math-chemistry majors, 4 double biology-math majors, 53 double biology-chemistry majors, 5 double biology-anthropology majors, and no other double majors?*

Exercise 31.2. *How many bit strings of length 15 start with the string 1111, end with the string 1000 or have 4th through 7th bits 1010?*

Exercise 31.3. *How many positive integers between 1000 and 9999 inclusive are divisible by any of 4, 10 or 25 (careful!)?*

Exercise 31.4. *How many permutations of the digits 1, 2, 3, 4, 5, have at least one digit in its own spot? In other words, a 1 in the first spot, or a 2 in the second, etc. For example, 35241 is OK since it has a 4 in the fourth spot, and 14235 is OK, since it has a 1 in the first spot (and also a 5 in the fifth spot). But 31452 is no good. Hint: Let A_1 be the set of permutations that have 1 in the first spot, let A_2 be the set of permutations that 2 in the second spot, and so on.*

Exercise 31.5. *How many permutations of the digits 1, 2, 3, 4, 5 have no digit in its own spot?*

Problems

Problem 31.1. *The membership of a language club consists of seven people who speak only English, eight speak only French, five speak only Spanish, seven speak only English and Spanish, two speak only French and Spanish, there are none who speak only English and French, and there are four who speak all three languages. How many members are in the club?*

Problem 31.2. *How many integers between 1 and 10000 (inclusive) are divisible by at least one of 9, 10, or 11?*

Problem 31.3. *Suppose p, q are two different primes. How many integers between 1 and the product pq are relatively prime to pq (or, same thing, how many are divisible by neither of p and q)? (The correct answer will factor neatly.)*

Problem 31.4. *Suppose p, q, r are three different primes. How many integers between 1 and the product pqr are relatively prime to pqr (or, same thing, how many are divisible by none of p, q and r)? (The correct answer will factor neatly.)*

Problem 31.5. *Suppose p, q, r, s are four different primes. How many integers between 1 and the product $pqrs$ are relatively prime to $pqrs$ (or, same thing, how many are divisible by none of p, q, r and s)? (The correct answer will factor neatly.)*

Problem 31.6. *Based on the results of the previous three problems, can you guess the neat formula for five, six, seven, and so on, different primes?*

Problem 31.7. *Of the words of length ten using the alphabet $\Sigma = \{a, b, c\}$, how many either begin abc or end cba or have $ccccc$ as the middle six letters?*

Problem 31.8. *There are $6!$ permutations of the numbers 1, 2, 3, 4, 5, 6. In some of these there is a run of three (or more) consecutive numbers that increase (left to right) such as 514632 which has the increasing run 146. Others do not have any increasing runs of length three such as (a cheap example) 654321 and (not quite as cheap) 615243. How many of the $6!$ permutations contain no increasing runs of length three (or more)? (Hint: runs of length three can start with the first, second, third, or fourth spot in the permutation.)*

Chapter 32: The Pigeonhole Principle

The pigeonhole principle, like the addition and multiplication principles, is another obvious counting fact. It is also called Dirichlet's box principle. The statement is simple: If $n + 1$ objects are divided into n piles (some piles can be empty), then at least one pile must have two or more objects in it. Or, more colorfully, if $n + 1$ pigeons land in n pigeonholes, then at least one pigeonhole has two or more pigeons. What could be more obvious? The pigeonhole principle is used to show that no matter how a certain task is carried out, some specific result must always happen.

As a simple example, suppose we have a drawer containing ten identical black socks and ten identical white socks. How many socks do we need to select to be sure we have a matching pair? The answer is three. Think of the pigeonholes as the colors black and white, and as each sock is selected put it in the pigeonhole of its color. After we have placed the third sock, one of the two pigeonholes must have at least two socks in it, and we will have a matching pair. Of course, we may have been lucky and had a pair after picking the second sock, but the pigeonhole principle *guarantees* that with the third sock we will have a pair.

As another example, suppose license plates are made consisting of four digits followed by two letters. Are there enough license plates for a state with seven million cars? No, since there are only $10^4 \cdot 26^2 = 6760000$ possible license plates, and so, by the pigeonhole principle, at least two of the seven million plates assigned would have to be the same.

A slightly fancier version of the pigeonhole principle says that if N objects are distributed in k piles, then there must be a least one pile with $\lceil N/k \rceil$ objects in it.

That formula looks impressive, but is easy to understand. For example, if there are 52 people in a room, we can be certain that there are at least eight born on the same day of the week. Think of it this way: with 49 people, it would be possible to have seven born on each of the seven days of the week. But when the 50th one is reached, it must boost one day up to an eighth person. That is really about all there is to it. The general proof of the fancy pigeonhole principle uses this same sort of reasoning.

Theorem 32.1 (Pigeonhole Principle). *If N objects are distributed in k piles, then there must be at least one pile with $\lceil N/k \rceil$ objects in it.*

Proof. Suppose by way of contradiction that we have N objects distributed in k piles, and suppose that every pile has fewer than $\lceil N/k \rceil$ objects in it. That means that each of the piles each contain $\lceil N/k \rceil - 1$ or fewer objects. We will use the fact the $\lceil N/k \rceil < \left(\frac{N}{k}\right) + 1$ to complete the proof. The total number of objects will be at most $k \left(\left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \left(\left(\frac{N}{k} + 1 \right) - 1 \right) = N$. That is a contradiction since we know there is a total of N objects in the k piles. ■

Even though the pigeonhole principle sounds very simple, clever applications of it can produce totally unexpected results.

Example 32.2. Five misanthropes move to a perfectly square deserted island that measures two kilometers on each side. Of course, being misanthropes, they want to live as far from each other as possible. Show that, no matter where they build on the island, some two will be no more than $\sqrt{2}$ kilometers of each other.

Solution. Divide the island into four one kilometer by one-kilometer squares by drawing lines joining the midpoints of opposite sides. Since there are five people and four squares, the pigeonhole principle guarantees there will be two people living in one of those four squares. But people in one of those squares cannot be further apart than the length of the diagonal of the square which is $\sqrt{2}$ by the Pythagorean Theorem.

Example 32.3. For any positive integer n , there is a positive multiple of n made up of a number of 1's followed by a number of 0's. For example, if $n = 1084$, we see $1084 \cdot 1025 = 1111100$.

Solution. Consider the $n + 1$ integers $1, 11, 111, \dots, 11 \dots 1$, where the last item consists of 1 repeated $n + 1$ times. Some two of these must be the same modulo n , and so n will divide the difference of those two. But the difference of two of those numbers is of the required type.

Example 32.4. Bill has 20 days to prepare his tiddlywinks title defense. He has decided to practice at least one hour every day. But, to avoid burn-out, he will not practice more than a total of 30 hours. Show there is a sequence of consecutive days during which he practices exactly 9 hours.

Solution. For $j = 1, 2, \dots, 20$, let t_j be the total number of hours Bill practices up to and including day j . Since he practices at least one hour every day, and the total number of hours is no more than 30, we see that $0 < t_1 < t_2 < \dots < t_{20} \leq 30$.

Add 9 to each term in this string of inequalities to get

$$9 < t_1 + 9 < t_2 + 9 < \dots < t_{20} + 9 \leq 39.$$

Thus, we have a total of forty integers (the t_i 's and $(t_i + 9)$'s) all between 1 and 39. By the Pigeonhole Principle some two must be equal. Since it can't be two t_i 's nor two $(t_i + 9)$'s we must have $t_i = t_j + 9$ for some i and j . It follows that $|t_j - t_i| = 9$. But this is the number of hours Bill practiced between the two days.

Example 32.5. One of the most important applications of the Pigeonhole Principle has to do with functions with finite domain and codomain. One can show that a function f from an n -set to an m -set is only if $n \leq m$ and onto only if $m \leq n$. Thus, a function from an n -set to an m -set is bijective if and only if $n = m$.

Exercises

Exercise 32.1. *Show that in any group of eight people, at least two were born on the same day of the week.*

Exercise 32.2. *Show that in any group of 100 people, at least 15 were born on the same day of the week.*

Exercise 32.3. *How many cards must be selected from a deck to be sure that at least six of the selected cards have the same suit?*

Exercise 32.4. *Show that in any set of n integers, where $n \geq 2$, there must be a pair with a difference that is a multiple of $n - 1$.*

Exercise 32.5. *Al has 75 days to master discrete mathematics. He decides to study at least one hour every day, but no more than a total of 125 hours. Show there must be a sequence of consecutive days during which he studies exactly 24 hours.*

Exercise 32.6. *Show that in any set of 217 integers, there must be a pair with a difference that is a multiple of 216.*

Problems

Problem 32.1. *Show that in a town with population 18,000, there must be at least two people with the same three initials.*

Problem 32.2. *What is the smallest town population that will guarantee there will be at least two people with the same three initials?*

Problem 32.3. *What is the smallest town population that will guarantee there will be at least five people with the same three initials?*

Problem 32.4. *How many cards have to be selected from a 52 card deck to be sure there will be two cards of the same suit?*

Problem 32.5. *How many cards have to be selected from a 52 card deck to be sure there will be two cards of the same rank?*

Problem 32.6. *Five misanthropes buy a six mile by eight mile rectangular plot in the arctic. Show that no matter where they build their houses, there will be at least two people that are no more than five miles apart. (You can assume the ice sheet they buy is perfectly flat.)*

Problem 32.7. *In any list of n integers, there will be a chunk of consecutive entries from the list that add up to a multiple of n . For example: in the list $-8, 4, 22, -11, 7$, we have that the combination $4 + 22 - 11 = 15$ is a multiple of 5.*

Problem 32.8. *Suppose $a_1, a_2, \dots, a_{99}$ is a permutation of $1, 2, \dots, 99$. Show that the product $(a_1 + 1)(a_2 + 2)(a_3 + 3) \cdots (a_{99} + 99)$ must be even.*

Problem 32.9. *In a rematch, Bill has 30 days to train for a new defense of his tiddlywinks title. He plans to practice at least one hour every day, but no more than 45 hours total. Show there is a sequence of consecutive days during which he practices exactly 14 hours.*

Chapter 33: Tougher Counting Problems

The counting exercises you've been asked to complete so far have not been realistic. In general, it won't be true that a counting problem fits neatly into a section. So, we need to work on the bigger picture.

When we start any counting exercise it is true that there is an underlying exercise at the basic level that we want to consider first. So instead of answering the question immediately we might first want to decide on what type of exercise we have. So far, we have seen three types which are distinguishable by the answers to two questions.

- (1) In forming the objects we want to count, is repetition allowed?
- (2) In forming the objects we want to count, does the order of selection matter?

The three scenarios we have seen so far are described in table [33.1](#).

Order	Repetition	Type	Form
Y	Y	r -strings	n^r
Y	N	r -permutations	$P(n, r)$
N	N	r -combinations	$\binom{n}{r}$

Table 33.1: Basic Counting Problems

There are two problems to address. First, table [33.1](#) is incomplete. What about, for example, counting objects where repetition is allowed, but order doesn't matter. Second, there are connections among the types which make some solutions appear misleading. But as a general rule of thumb, if we correctly identify the type of problem we are working on, then all we have to do is use the principles of addition, multiplication, inclusion/exclusion, or exclusion to decompose our problem into subproblems. The solutions to the subproblems often have the same form as the underlying problem. The principles we employed direct us on how the sub-solutions should be re-combined to give the final answer.

Example 33.1. *As an example of the second problem, if we ask how many binary strings of length 10 contain exactly three 1's, then the underlying problem is an r -string problem. But in this case the answer is $\binom{10}{3}$. Of course this is really $\binom{10}{3}1^31^7$ from the binomial theorem. In this case the part of the answer that looks like n^r is suppressed since it's trivial. To see the difference we might ask how many ternary strings of length 10 contain exactly three 1's. Now the answer is $\binom{10}{3}1^32^7$ since we choose the three positions for the 1's, and then fill in each of the 7 remaining positions with a 0 or a 2.*

To begin to address the first problem we introduce the **basic donut shop problem**: If you get to the donut shop before the cops get there, you will find that they have a nice variety of donuts. You might want to order several dozen. They will put your order in a box. You don't particularly care what order the donuts are put into the box. You do usually want more than one of several

types. The number of ways for you to complete your order is therefore a counting problem where order doesn't matter, and repetition is allowed.

In order to answer the question of how many ways you can complete your order, we first recast the problem mathematically. From among n types of objects we want to select r objects. If x_i denotes the number of objects of the i th type selected, we have $0 \leq x_i$, (since we cannot choose a negative number of chocolate donuts), also $x_i \in \mathbb{Z}$, (since we cannot select fractional parts of donuts). So, the different ways to order are in one-to-one correspondence with the solutions to

$$x_1 + x_2 + \cdots + x_n = r, \text{ with } x_i \geq 0, x_i \in \mathbb{Z}, \text{ for } i = 1, 2, \dots, n.$$

In order to compute the number of solutions in non-negative integers to $x_1 + \cdots + x_n = r$, we model each solution as a string (possibly empty) of x_1 1's followed by a +, then a string of x_2 1's followed by a +, ... then a string of x_{n-1} 1's followed by a +, then a string of x_n 1's. So, for example, if $x_1 = 2, x_2 = 0, x_3 = 1, x_4 = 3$ is a solution to $x_1 + x_2 + x_3 + x_4 = 6$ the binary string we get is 11 + +1 + 111. Notice the empty string of 1's between the first two +'s indicating that $x_2 = 0$.

Thus, we see that the total number of solutions in non-negative integers to $x_1 + \cdots + x_n = r$, is the number of binary strings of length $r + n - 1$ with exactly r 1's and $(n - 1)$ +'s. From the remark above, the number of ways to select r donuts from n different types is

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

The basic donut shop problem is not very realistic in two ways. First it is common that some of your order will be determined by other people. You might for example canvass the people in your office before you go to see if there is anything you can pick up for them. So, whereas you want to order r donuts, you might have been asked to pick up a certain number of various types.

Now suppose that we know that we want to select r donuts from among n types so that at least a_i ($a_i \geq 0$) donuts of type i are selected. The formulation is now $x_1 + x_2 + \cdots + x_n = r$, where $a_i \leq x_i$, and $x_i \in \mathbb{Z}$. Set $y_i = x_i - a_i$ for $i = 1, 2, \dots, n$, and $a = a_1 + a_2 + \cdots + a_n$. This change of variables gives $0 \leq y_i, y_i \in \mathbb{Z}$ and

$$\sum_{i=1}^n y_i = \sum_{i=1}^n x_i - a_i = \left[\sum_{i=1}^n x_i \right] - \left[\sum_{i=1}^n a_i \right] = r - a.$$

So, the number of ways to complete our order is $\mathcal{C}(n + (r - a) - 1, r - a)$.

Still, we qualified the donut shop problem by supposing that we arrived before the cops did.

If we arrive at the donut shop after canvassing our friends, we want to select r donuts from among n types. The problem is that if the cops have already been there, there are probably only a few donuts left of each type. This may place an upper limit on how often we can select a particular type. So now we wish to count solutions to

$$x_1 + x_2 + \cdots + x_n = r \text{ with } a_i \leq x_i \leq b_i, x_i \in \mathbb{Z}.$$

We proceed by replacing r with $s = r - a$, where a is the sum of lower bounds. We also replace b_i with $c_i = b_i - a_i$ for $i = 1, 2, \dots, n$. So, we want to find the number of solutions with

$$0 \leq y_i \leq c_i, y_i \in \mathbb{Z} \text{ and } y_1 + y_2 + \dots + y_n = s.$$

There are now several ways to proceed. We will choose inclusion/exclusion in the second form. Let $\mathcal{U}$ be the set of all solutions in nonnegative integers to $y_1 + y_2 + \dots + y_n = s$. Next, let A_i denote those solutions to $y_1 + y_2 + \dots + y_n = s$ with $c_i < y_i$. Realize that because $c_i, y_i \in \mathbb{Z}$ that $c_i < y_i$ is equivalent to $c_i + 1 \leq y_i$. We want to compute $|\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}|$.

Example 33.2. *Let us count the number of solutions to*

$$x_1 + x_2 + x_3 + x_4 = 34$$

where $0 \leq x_1 \leq 4, 0 \leq x_2 \leq 5, 0 \leq x_3 \leq 8$, and $0 \leq x_4 \leq 40$.

As discussed above we have $c_1 = 4, c_2 = 5, c_3 = 8$, and $c_4 = 40$. Hence we see that

$$|\mathcal{U}| = \binom{34 + 4 - 1}{34}.$$

Now A_i will denote the solutions in nonnegative integers to

$$x_1 + x_2 + x_3 + x_4 = 34, \text{ with } x_i > c_i, i = 1, 2, 3, 4.$$

Next realize that $A_4 = \emptyset$, so $\overline{A_4} = \mathcal{U}$ and $\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \overline{A_4} = \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$.

Now to compute $|A_1|$, we must first rephrase $x_1 > 4$ as a non-strict inequality, i.e. $5 \leq x_1$. So it follows that

$$|A_1| = \binom{29 + 4 - 1}{29}.$$

Similarly,

$$|A_2| = \binom{28 + 4 - 1}{28} \text{ and } |A_3| = \binom{25 + 4 - 1}{25}.$$

Next, we observe that $A_1 \cap A_2$ represents all solutions in nonnegative integers to

$$x_1 + x_2 + x_3 + x_4 = 34 \text{ with } 5 \leq x_1 \text{ and } 6 \leq x_2.$$

So we have that

$$|A_1 \cap A_2| = \binom{23 + 4 - 1}{23}.$$

Also, we find that

$$|A_1 \cap A_3| = \binom{20+4-1}{20} \text{ and } |A_2 \cap A_3| = \binom{19+4-1}{19}.$$

Finally, we see that

$$|A_1 \cap A_2 \cap A_3| = \binom{14+4-1}{14}.$$

Hence, the final answer is

$$\begin{aligned} |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \overline{A_4}| &= \binom{34+4-1}{34} - \binom{29+4-1}{29} - \binom{28+4-1}{28} - \binom{25+4-1}{25} \\ &\quad + \binom{23+4-1}{23} + \binom{20+4-1}{20} + \binom{19+4-1}{19} - \binom{14+4-1}{14}. \end{aligned}$$

We leave the answer in this form for clarity. The numerical value is not illuminating.

We can now solve general counting exercises where order is unimportant and repetition is restricted somewhere between no repetition, and full repetition.

To complete the picture, we should be able to also solve counting exercises where order is important and repetition is partial. This is somewhat easier. It suffices to consider the sub-cases in example [33.3](#).

Example 33.3. Let us take as initial problem the number of quaternary strings of length 15. There are 4^{15} of these.

Now, if we ask how many contain exactly two 0's, the answer is

$$\binom{15}{2} 3^{13}.$$

If we ask how many contain exactly two 0's and four 1's, the answer is

$$\binom{15}{2} \binom{13}{4} 2^9.$$

And, if we ask how many contain exactly two 0's, four 1's and five 2's, the answer is

$$\binom{15}{2} \binom{13}{4} \binom{9}{5} \binom{4}{4} = \frac{15!}{2! 4! 5! 4!}.$$

So, in fact many types of counting are related by what we call the multinomial theorem.

Theorem 33.4. When r is a nonnegative integer and $x_1, x_2, \dots, x_n \in \mathbb{R}$, then

$$(x_1 + x_2 + \dots + x_n)^r = \sum_{\substack{e_1+e_2+\dots+e_n=r \\ 0 \leq e_i, e_i \in \mathbb{Z}}} \binom{r}{e_1, e_2, \dots, e_n} x_1^{e_1} x_2^{e_2} \dots x_n^{e_n} \text{ where } \binom{r}{e_1, e_2, \dots, e_n} = \frac{r!}{e_1! e_2! \dots e_n!}.$$

To recap, when we have a counting exercise, we should first ask whether order is important and then ask whether repetition is allowed. This will get us into the right ballpark as far as the form of the solution. We must use basic counting principles to decompose the exercise into sub-problems. Solve the sub-problems and put the pieces back together. Solutions to sub-problems usually take the same form as the underlying problem, though they may be related to it via the multinomial theorem. Table [33.2](#) synthesizes our six fundamental cases.

Order	Repetition	Form
Yes	Yes	n^r
Yes	No	$P(n, r)$
No	Yes	$C(r, r + n - 1)$
No	No	$C(n, r)$
Yes	some	$C(r; k_1, k_2, \dots, k_n)$
No	some	$C(r, r + n - 1), \text{ w/ I/E}$

Table 33.2: Six Counting Problems

Exercises

Exercise 33.1. *How many quaternary strings of length n are there (a quaternary string uses 0's, 1's, 2's, and 3's)?*

Exercise 33.2. *How many quaternary strings of length less than or equal to 7 are there?*

Exercise 33.3. *How many solutions in integers are there to*

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 54, \text{ where } 3 \leq x_1, 4 \leq x_2, 5 \leq x_3, \text{ and } 6 \leq x_4, x_5, x_6, x_7?$$

Exercise 33.4. *How many ternary strings of length n start 0101 and end 212?*

Exercise 33.5. *A doughnut shop has 8 kinds of doughnuts: chocolate, glazed, sugar, cherry, straw- berry, vanilla, caramel, and jalapeño. How many ways are there to order three dozen doughnuts, if at least 4 are jalapeño, at least 6 are cherry, and at least 8 are strawberry, but there are no restrictions on the other varieties?*

Exercise 33.6. *How many strings of twelve lowercase English letters are there*

- (a) *which start and end with the letter x , if letters can be repeated?*
- (b) *which contain the letter x exactly once, if letters can be repeated?*
- (c) *which contain each of the letters x and y exactly once, if letters can be repeated?*
- (d) *which contain at least one letter from the first half of the alphabet (a through m), where letters may be repeated?*

Exercise 33.7. *How many bit strings of length 19 either begin 0101, or have 4th, 5th and 6th digits 101, or end 1010?*

Exercise 33.8. *How many pentary strings (i.e. strings using the digits 0,1,2,3,4) of length 15 consist of three 0's, four 1's, three 2's, four 3's and one 4?*

Exercise 33.9. *Seven lecturers and fourteen professors are on the faculty of a math department.*

- (a) *How many ways are there to form a committee with seven members which contains more lecturers than professors?*
- (b) *How many ways are there to form a committee with seven members where the professors outnumber the lecturers by at least a two-to-one margin?*
- (c) *How many ways are there to form a committee with seven members consisting of at least five lecturers?*

Exercise 33.10. *In how many ways can twenty people form a line at a ticket window if Hans and wife Brunhilda are having a spat, and refuse to stand in consecutive places in the line?*

Exercise 33.11. *Prove that a set with $n \geq 1$ elements has the same number of subsets with an even number of elements, as subsets with an odd number of elements.*

Problems

Problem 33.1. *A doughnut shop has 8 kinds of doughnuts: chocolate, glazed, sugar, cherry, straw- berry, vanilla, caramel, and jalapeño. How many ways are there to order three dozen doughnuts, if at most 4 are jalapeño, at most 6 are cherry, and at most 8 are strawberry, but there are no restrictions on the other varieties?*

Problem 33.2. *How many strings of twelve lowercase English letters are there*

- (a) *which start with the letter x, if letters may be repeated?*
- (b) *which contain the letter x at least once, if letters can be repeated?*
- (c) *which contain each of the letters x and y at least once, if letters can be repeated?*
- (d) *which contain at least one vowel, where letters may not be repeated?*

Problem 33.3. *How many ternary string of length 9 have*

- (a) *exactly four 1's?*
- (b) *at least three 0's?*
- (c) *at most three 1's?*
- (d) *exactly four 0's, three 1's? and two 2's?*

Problem 33.4. *How many ways are there to seat six people at a circular table where two seatings are considered equivalent if one can be obtained from the other by rotating the table?*

Problem 33.5. *A donut shop sells six types of donut. You buy a scratch-off ticket that promises you will win anywhere from one to two dozen donuts. How many different prizes are possible?*

Problem 33.6. *How many ternary strings of length n contain no two adjacent identical symbols? Examples: ($n = 8$) 13123231 is good, but 13112321 is bad.*

Problem 33.7. *How many ternary strings of length n contain at least two adjacent identical symbols? Examples: ($n = 9$) 131212321 is bad, but 131123321 is good.*

Chapter 34: Counting Using Recurrence Relations

It is not always convenient to use the methods of earlier chapters to solve counting problems. Another technique for finding the solution to a counting problem is **recursive counting**. The method will be illustrated with several examples.

Example 34.1. Recall that a bit string is a list of 0's and 1's, and the length of a bit string is the total number of 0's and 1's in the string. For example, 10111 is a bit string of length five, and 000100 is a bit string of length six. The problem of counting the number of bit strings of length n is duck soup. There are two choices for each bit, and so, applying the multiplication principle, there are 2^n such strings. However, consider the problem of counting the number of bit strings of length n with no adjacent 0's.

Let's use a_n to denote the number of bit strings of length n with no adjacent 0's. Here are a few sample cases for small values of n .

- **$n = 0$:** Just one good bit string of length zero, and that is λ , the empty bit string. So $a_0 = 1$.
- **$n = 1$:** There are two good bit strings of length one. Namely 0 and 1. So $a_1 = 2$.
- **$n = 2$:** There are three good bit strings of length two. Namely, 01, 10 and 11. (Of course, 00 is a bad bit string.) That means $a_2 = 3$.
- **$n = 3$:** Things start to get confusing now. But here is the list of good bit strings of length three: 010, 011, 101, 110, and 111. So $a_3 = 5$.
- **$n = 4$:** A little scratch work produces the good bit strings 0101, 0111, 1011, 1101, 1111, 0110, 1010, and 1110, for a total of eight. That means $a_4 = 8$.

We can do a few more, but we might not recognize a pattern to produce a formula for a_n like the 2^n formula that gives the total number of all bit strings of length n . Even though a formula for a_n might not be apparent, there is a pattern to the list of values for a_n which looks like the Fibonacci sequence pattern. In fact, the list so far looks like 1, 2, 3, 5, 8, and if a few more are worked out by brute force, it turns out the list continues 13, 21, 34. So, it certainly seems that the solution to the counting problem can be expressed recursively as $a_0 = 1$, $a_1 = 2$, and for $n \geq 2$, $a_n = a_{n-1} + a_{n-2}$. If this guess is correct, then we can compute the number of good bit strings of length n . We just calculate a_0 , a_1 , a_2 , etc., until we reach the a_n we are interested in.

Such a recursive solution to counting problems is certainly less satisfactory than a simple formula, but some counting problems are so messy that a simple formula might not be possible, and the recursive solution is better than nothing in such a case.

There is a problem with the recursive solution proffered in example [34.1](#). We said that *it seems that* the solution to the counting problem can be expressed recursively as $a_0 = 1$, $a_1 = 2$, and for

$n \geq 2$, $a_n = a_{n-1} + a_{n-2}$. That *it seems that* is not an acceptable justification of the formula. After all, we are basing that guess on just eight or ten values of the infinite sequence a_n , and it is certainly possible that those values happen to follow the pattern we've guessed simply by accident. Maybe the true pattern is much more complicated, and we have been tricked by the small number of cases we have considered. It is necessary to show that the guessed pattern is correct by supplying a logical argument.

Our argument would begin by checking the initial conditions we offered. In other words, we would verify by hand that $a_0 = 1$ and $a_1 = 2$. This serves as a basis for the verification of the recursive formula. Now what we want to do is assume that we have already calculated all the values $a_0, a_1, \dots, a_k$ for some $k \geq 1$, and **show** that a_{k+1} must equal $a_k + a_{k-1}$. It is very important to understand that *we do not want to compute the value of a_{k+1} . We only want to prove that $a_{k+1} = a_k + a_{k-1}$* . The major error made doing these types of problems is attempting to compute the specific value of a_{k+1} . **Don't fall for that trap!** After all, if it were possible to actually compute the specific value of a_{k+1} , then we could find a formula for a_n in general, and we wouldn't have to be seeking a recursive relation at all.

Consider the following argument would for the bit string example. Suppose we have lists of the good bit strings of lengths $0, \dots, k$. Here is how to make a list of all the good bit strings of length $k + 1$. First, take any good bit string of length k and add a 1 on the right-hand end. The result must be a good bit string of length $k + 1$ (since we added a 1 to the end, and the original bit string didn't have two consecutive 0's, the new bit string cannot have two consecutive 0's either). In that way we form some good bit strings of length $k + 1$. In fact, we have built exactly a_k good bit strings of length $k + 1$. But wait, there's more! (as they say in those simple-minded TV ads). Another way to build a good bit string of length $k + 1$ is to take a good bit string of length $k - 1$ and add 10 to the right end. These will also be good bit strings of length $k + 1$. And these all end with a 0, so they are all new ones, and not ones we built in the previous step. How many are there of this type? One for each of the good bit strings of length $k - 1$, or a total of a_{k-1} . Thus, we have built $a_k + a_{k-1}$ good bit strings of length $k + 1$. Now we will show that in fact we have a complete list of all good bit string of length $k + 1$, and that will complete the proof that $a_{k+1} = a_k + a_{k-1}$. But before driving that last nail into the coffin, let's look at the steps outlined above for the case $k + 1 = 4$.

The previous paragraph provides an algorithm for building good bit strings of length $k + 1$ from good bits strings of lengths k and $k - 1$. The algorithm instructs us to add 1 to the right end of all the good bit strings of length k and 10 to the right of all the good bit strings of length $k - 1$. Applying the algorithm for the case $k + 1 = 4$, gives the following list, where the added bits are put in parentheses to make them stand out. 010(1), 011(1), 101(1), 110(1), 111(1), 01(10), 10(10), and 11(10).

There remains one detail to iron out. The algorithm will produce good bit strings of length $k + 1$. But, does it produce *every* good bit string of length $k + 1$? If it does not, then the recursive relation we are offering for the solution to the counting problem will eventually begin to produce answers that are too small, and we will undercount the number of good bit strings.

To see that we do count all good bit strings of length $k + 1$, consider an arbitrary good bit string of length $k + 1$, call it s for short, and look at the right most bit of s . There are two possibilities for that bit. It could be a 1. If that is so, then when the 1 is removed the remaining bit string is a good string of length k (it can't have two adjacent 0's since s doesn't have two adjacent 0's). That means the bit string s is produced by adding a 1 to the right end of a good bit string of length k , and so s is produced by the first step in the algorithm. The other option for s is that the right most bit is a 0. But then the second bit in from the right must be a 1, since s is a good bit string, so it doesn't have adjacent 0's. So the last two bits on the right of s are 10. If those two bits are removed, there remains a good bit string of length $k - 1$. Thus s is produced by adding 10 to the right end of a good bit string of length $k - 1$, and so s is produced by the second case in the algorithm.

In a nutshell, we have shown our algorithm produces $a_k + a_{k-1}$ good bit strings of length $k + 1$, and that the algorithm does not miss any good bit strings of length $k + 1$. Thus we have proved that $a_{k+1} = a_k + a_{k-1}$ for all $k \geq 2$.

Example 34.1 was explained in excruciating detail. Normally, the verifications will be much more briefly presented. It takes a while to get used to recursive counting, but once the light goes on, the beauty and simplicity of the method will become apparent.

A more efficient explanation of the bit string example runs as follows: Let A_k denote the set of bit strings of length k with no adjacent 0's. Then $a_k = |A_k|$. We have $a_0 = 1$ and $a_1 = 2$ by brute-force enumeration. Consider then $x \in A_k$ for some $k \geq 2$. Either x starts with a 1, in which case $x = 1y$ where $y \in A_{k-1}$. Or (exclusively) x starts with a 0. In this case the next bit in x must be 1 so $x = 01z$ where $z \in A_{k-2}$. This covers all possibilities so by the addition principle

$$a_k = a_{k-1} + a_{k-2}, \text{ for } k \geq 2 \text{ and } a_0 = 1, a_1 = 2.$$

Example 34.2. *This example is a little silly since it is very easy to write down a formula to solve the counting problem. But the point of the example is not to find the solution to the problem but rather to exhibit recursive counting in action. The problem is to compute the total number of individual squares on an $n \times n$ checkerboard. If we let the total number of squares be denoted by s_n , then obviously $s_n = n^2$. For example, an ordinary checkerboard is an 8×8 board, and it has a total of $s_8 = 8^2 = 64$ individual squares. But let's count the number of squares recursively. Clearly $s_0 = 0$. Now suppose we have computed the values of $s_0, s_1, \dots, s_k$, for some $k \geq 0$. We will show how to compute s_{k+1} from those known values. To determine s_{k+1} , draw a $(k + 1) \times (k + 1)$ checkerboard (make a sketch of such a board for say $k + 1 = 5$ so you can follow the process described nex.). From that $(k + 1) \times (k + 1)$ board, slice off the right hand column of squares, and the bottom row of squares. What is left over will be a $k \times k$ checkerboard, so it will have s_k individual squares. That means that*

$$s_{k+1} = s_k + \text{the number of squares sliced off}$$

Now ignore the lower right hand corner square for a moment. There are k other squares in the right-hand column that were sliced off. Likewise, ignoring the corner square, there are k other

squares in the bottom row that were sliced off. Hence the total number of squares sliced off was $k + k + 1$, the 1 accounting for the corner square. Thus

$$s_{k+1} = s_k + k + k + 1 = s_k + 2k + 1, \text{ for } k \geq 0.$$

So a recursive solution to the problem of counting s_n = number of individual squares on an $n \times n$ checkerboard is

$$s_0 = 0 \text{ and } s_m = s_{m-1} + 2m + 1, \text{ for } m \geq 1.$$

Using the recursive relation, we get $s_0 = 0$, $s_1 = s_0 + 2 \cdot 0 + 1 = 0 + 0 + 1 = 1$, followed by $s_2 = s_1 + 2 \cdot 1 + 1 = 1 + 2 + 1 = 4$, $s_3 = s_2 + 2 \cdot 2 + 1 = 4 + 4 + 1 = 9$, and so on, giving what we recognize as the correct answers.

Example 34.3. Suppose we have available an unlimited number of pennies and nickels to deposit in a vending machine (a really old vending machine it seems, since it even accepts pennies). Let d_n be the number of different ways of depositing a total of n cents in the machine. Just to make sure we understand the problem, let's compute d_n for a few small values of n . Clearly $d_0 = 1$ since there is only one way to deposit no money in the machine (namely don't put any money in the machine!). $d_1 = 1$ (put in one penny), $d_2 = 1$ (put in two pennies), $d_3 = 1$ (put in three pennies), $d_4 = 1$ (put in four pennies). Now things start to get exciting! $d_5 = 2$ (put in five pennies or put in one nickel). And even more thrilling is $d_6 = 3$ (the three options are (1) six pennies, (2) one penny followed by a nickel, and (3) one nickel followed by a penny). That last count indicates a fact that may not have been clear: the order on which pennies and nickels are deposited is considered important. With a little more trial and error with pencil and paper, further values are found to be $d_7 = 4$, $d_8 = 5$, $d_9 = 6$, $d_{10} = 8$, $d_{11} = 11$, and $d_{12} = 15$. It is hard to see a closed formula for these values. But it is relatively easy to write down a recursive relation that produces this sequence of values. Think of it this way, suppose we wanted to put n cents in the machine, where $n \geq 5$. We can make the first coin either a penny or a nickel. If we make the first coin a penny, then we will need to add $n - 1$ more cents, which can be done in d_{n-1} ways. On the other hand, if we make the first coin a nickel, we will need to deposit $n - 5$ more cents, and that can be done in d_{n-5} ways. By the addition principle we conclude that the number of ways of depositing n cents is $d_{n-1} + d_{n-5}$. That is, $d_n = d_{n-1} + d_{n-5}$ for $n \geq 5$.

Since our recursive relation for d_n does not kick in until n reaches 5, we will need to include d_0 , d_1 , d_2 , d_3 , and d_4 as initial terms. So, the recursive solution to this counting problem is

$$d_n = d_{n-1} + d_{n-5} \text{ for } n \geq 5 \text{ with } d_0 = d_1 = d_2 = d_3 = d_4 = 1.$$

Example 34.4 (The Tower of Hanoi). The classic example of recursive counting concerns the story of the Tower of Hanoi. A group of monks wished a magical tower to be constructed from 1000 stone rings. The rings were to be of 1000 different sizes. The size and composition of the rings was to be designed so that any ring could support the entire weight of all of the rings smaller than itself, but each ring would be crushed beneath the weight of any larger ring.

The monks hired the lowest bidder to construct the tower in a clearing in the dense jungle nearby. Upon completion of construction the engineers brought the monks to see their work. The

monks admired the exquisite workmanship but informed the engineers that the tower was not in the proper clearing.

In the jungle there were only three permanent clearings. The monks had labelled them A, B and C. The engineers had labelled them in reverse order. The monks instructed the engineers to move the tower from clearing A to clearing C!

Because of the massive size of the rings, the engineers could only move one per day. No ring could be left anywhere in the jungle except one of A, B, or C. Lastly, each clearing was only large enough so that rings could be stored there by stacking them one on top of another.

The monks then asked the engineers how long it would take for them to fix the problem.

Before they all flipped a gasket, the most mathematically talented engineer came upon the following solution.

Let H_n denote the minimum number of days required to move an n ring tower from A to C under the constraints given. Then $H_1 = 1$, and in general an n ring tower can be moved from A to C by first moving the top $(n - 1)$ rings from A to B leaving the bottom ring at A. Then moving the bottom ring from A to C. Then moving the top $(n - 1)$ rings from clearing B to clearing C. That shows $H_n \leq 2 \cdot H_{n-1} + 1$, for $n \geq 2$, and a little more thought shows the algorithm just described cannot be improved upon. Thus $H_n = 2 \cdot H_{n-1} + 1$ for $n \geq 2$.

Using the initial condition $H_1 = 1$ together with the recursive relation $H_n = 2 \cdot H_{n-1} + 1$, we can generate terms of the sequence:

$$1, 3, 7, 15, 31, 63, 127, 255, 511, \dots$$

and it looks like $H_n = 2^n - 1$ for $n \geq 1$, which can be verified by an easy induction proof.

So, the problem would be fixed in $2^{1000} - 1$ days, or approximately 2.93564×10^{296} centuries. Now, that is job security!

Exercises

Here are a few general rules for solving counting problems recursively:

- (1) Do a few small cases by brute force.
- (2) Think recursively: how can a larger case be solved if the solutions to smaller cases are known.
- (3) Check the numbers produced by the recursive solution to make sure they agree with the values obtained by brute force.

Exercise 34.1. *On day zero, a piggy bank contains \$0. Each day, one more penny is added to the bank than the day before. So, on day 1, one penny is added, on day 2, two pennies are added. Write a recursive formula for the total number of pennies in the bank each day, $n = 0, 1, 2, \dots$.*

Exercise 34.2. *Al climbs stairs by taking either one or two steps at a time. For example, he can climb a flight of three steps in three different ways: (1) one step, one step, one step or (2) two step, one step, or (3) one step, two step. Determine a recursive formula for the number of different ways Al can climb a flight of n steps.*

Exercise 34.3. *Find a recurrence relation for the number of bit strings of length n that contain an even number of 0's.*

Exercise 34.4. *Find a recurrence relation for the number of bit strings of length n that contain two consecutive 0's.*

Exercise 34.5. *Find a recurrence relation for the number of bit strings of length n that contain the string 01.*

Exercise 34.6. *Find a recurrence relation for the number of ternary strings of length n that contain two consecutive 0's.*

Exercise 34.7. *Find a recurrence relation for the number of subsets of $\{1, 2, 3, \dots, n\}$ that do not contain any consecutive integers. Examples for $n = 9$: the subset $\{1, 3, 8\}$ is good, but the subset $\{2, 5, 6, 9\}$ is bad since it contains the consecutive integers 5, 6.*

Exercise 34.8. *Suppose in the original Tower of Hanoi problem there are four clearings A, B, C, D. Find a recursive relation for J_n , the minimum number of moves needed to transfer the tower from clearing A to clearing D.*

Problems

See the Chapter 34 Exercises page for a few general rules for solving counting problems recursively.

Problem 34.1. Suppose on December 31, 2000, a deposit of \$100 is made in a savings account that pays 10% annual interest (Ah, those were the days!). So, one year after the initial deposit, on December 31, 2001, the account will be credited with \$10 and have a value of \$110. On December 31, 2002 that account will be credited with an additional \$11 and have value \$121. Find a recursive relation that gives the value of the account n years after the initial deposit.

Problem 34.2. Sal climbs stairs by taking either one, two, or three steps at a time. Determine a recursive formula for the number of different ways Sal can climb a flight of n steps. In how many ways can Sal climb a flight of 10 steps?

Problem 34.3. Passwords for a certain computer system are strings of uppercase letters. A valid password must contain an even number of X's. Determine a recurrence relation for the number of valid passwords of length n .

Problem 34.4. A (cheap) vending machine accepts pennies, nickels, and dimes. Let d_n be the number of ways of depositing n cents in the machine where the order in which the coins are deposited matters. Determine a recurrence relation for d_n . Give the initial conditions.

Problem 34.5. Suppose the Tower of Hanoi rules are changed so that stones may only be transferred to an adjacent clearing in one move. Let I_n be the minimum number of moves required to transfer tower from clearing A to clearing C?

(a) By brute force determine I_1, I_2 and I_3 .

(b) Find a recursive relation for I_n .

(c) Guess a formula for I_n .

Problem 34.6. Find a recurrence relation for the number of binary strings of length n which do not contain the substring 010.

Problem 34.7. Find a recurrence relation for the number of ternary strings of length n that contain three consecutive zeroes.

Problem 34.8. Find a recurrence relation for the number of quaternary strings of length n which contain two consecutive 1's.

Problem 34.9. Let n be a positive integer. Find a recurrence relation that counts the number of increasing sequences of distinct integers that start with 1 and end with n . Example: For $n = 4$, there are 4 such sequences. They are 1, 4; 1, 2, 4; 1, 3, 4; and 1, 2, 3, 4.

Chapter 35: Solutions to Recurrence Relations

In chapter [34](#), it was pointed out that recursively defined sequences suffer from one major drawback: In order to compute a particular term in the sequence, it is necessary to first compute all the terms of the sequence leading up to the one that is wanted. Imagine the chore to calculate the 250th Fibonacci number, f_{250} ! For problems of computation, there is nothing like having a formula like $a_n = n^2$, into which it is merely necessary to plug-in the number of interest.

It may be possible to find a formula for a sequence that is defined recursively. When that can be done, you have the best of both the formula and recursive worlds. If we find a formula for the terms of a recursively defined sequence, we say we have **solved** the recursion.

Example 35.1. *Here is an example: The sequence $\{a_n\}$ is defined recursively by the initial condition $a_0 = 2$, and the recursive formula $a_n = 2a_{n-1} - 1$ for $n \geq 1$. If the first few terms of this sequence are written out, the results are*

$$2, 3, 5, 9, 17, 33, 65, 129, \dots$$

and it shouldn't be too long before the pattern becomes clear. In fact, it looks like $a_n = 2^n + 1$ is the formula for a_n where $n \geq 0$. You do have to recognize the slightly hidden powers of 2:

$$1, 2, 4, 8, 16, 32, 64, \dots$$

To prove that guess is correct, induction would be the best way to go. Here are the details. Just to make everything clear, here is what we are going to show: If $a_0 = 2$, and $a_n = 2a_{n-1} - 1$ for $n \geq 1$, then $a_n = 2^n + 1$ for all $n \geq 0$. The basis for the inductive proof is the case $n = 0$. The correct value for a_0 is 2, and the guessed formula has value 2 when $n = 0$, so that checks out. Now for the inductive step: suppose that $a_k = 2^k + 1$ for an arbitrary $k \geq 0$. We want to show $a_{k+1} = 2^{k+1} + 1$. Well, we know that $a_{k+1} = 2a_k - 1$ since $k + 1 \geq 1$. By substitution $a_{k+1} = 2(2^k + 1) - 1 = 2^{k+1} + 2 - 1 = 2^{k+1} + 1$, just as was to be proved. It can now be concluded that the formula we guessed is correct for all $n \geq 0$.

In example [35.1](#), it was possible to guess the correct formula for a_n after looking at a few terms. In most cases the formula will be so complicated that that sort of guessing will be out of the question.

There is a method that will almost always solve a simple recurrence of the form $a_0 = a$ and for, $n \geq 1$, $a_n = ba_{n-1} + c$ (where a, b, c are constants). The method is called **unfolding**.

Example 35.2. *Let's solve $a_0 = 2$ and, for $n \geq 1$, $a_n = 5 + 2a_{n-1}$. The plan is to write down the recurrence relation and then substitute for a_{n-1} , then for a_{n-2} , and so on, until we reach a_0 . It looks like this*

$$\begin{aligned} a_n &= 5 + 2a_{n-1} \\ &= 5 + 2(5 + 2a_{n-2}) = 5 + 5 \cdot 2 + 2^2 a_{n-2} \\ &= 5 + 5 \cdot 2 + 2^2(5 + 2a_{n-3}) = 5 + 5 \cdot 2 + 5 \cdot 2^2 + 2^3 a_{n-3}. \end{aligned}$$

If this substitution is continued, eventually we reach an expression we can compute in closed form:

$$\begin{aligned}a_n &= 5 + 5 \cdot 2 + 5 \cdot 2^2 + 5 \cdot 2^3 + \cdots + 5 \cdot 2^{n-1} + 2^n a_0 \\&= 5(1 + 2 + 2^2 + \cdots + 2^{n-1}) + 2^n \cdot 2 \\&= 5 \frac{2^n - 1}{2 - 1} + 2 \cdot 2^n \\&= 5(2^n - 1) + 2 \cdot 2^n \\&= 7 \cdot 2^n - 5.\end{aligned}$$

In the second to last step we use the formula for adding the terms of a geometric sequence.

Exercises

Exercise 35.1. *Guess the solution to $a_0 = 2, a_1 = 4$ and for $n \geq 2, a_n = 4a_{n-1} - 3a_{n-2}$ and prove your guess is correct by induction.*

Exercise 35.2. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 5a_{n-1}$.*

Exercise 35.3. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 5a_{n-1} + 3$. Hint: This one will involve applying the geometric sum formula.*

Problems

Problem 35.1. *Guess the solution to $a_0 = 1, a_1 = 5$ and for $n \geq 2, a_n = a_{n-1} + 2a_{n-2}$ and prove your guess is correct by induction.*

Problem 35.2. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 7a_{n-1}$.*

Problem 35.3. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 7a_{n-1} + 3$. Hint: This one will involve applying the geometric sum formula.*

Chapter 36: The Method of Characteristic Roots

There is no method that will solve all recurrence relations. However, for one type there is a standard technique. The type is called a **linear recurrence relation with constant coefficients**. In such a recurrence relation, the recurrence formula has the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n)$$

where $c_1, \dots, c_k$ are constants with $c_k \neq 0$, and $f(n)$ is any function of n .

The **degree** of the recurrence is k , the number of terms we need to go back in the sequence to compute each new term. If $f(n) = 0$, then the recurrence relation is called homogeneous. Otherwise, it is called **non-homogeneous**.

In chapter [35](#), we noted that some simple non-homogeneous linear recurrence relations with constant coefficients can be solved by unfolding. This method is not powerful enough for more general problems. In this chapter we introduce a basic method that, in principle at least, can be used to solve any homogeneous linear recurrence relation with constant coefficients.

We begin by considering the degree 2 case. That is, we have a recurrence relation of the form $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, for $n \geq 2$, where c_1, c_2 are real constants. We must also have two initial conditions a_0 and a_1 . That is, we are given a_0 and a_1 and the formula $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, for $n \geq 2$. Notice that $c_2 \neq 0$ or else we have a linear recurrence relation with constant coefficients and degree 1. What we seek is a **closed form formula** for a_n , which is a function of n alone, and which is therefore independent of the previous terms of the sequence.

Here's the technique in a specific example: The problem we will solve is to find a formula for the terms of the sequence

$$a_0 = 4, a_1 = 8 \text{ and } a_n = 4a_{n-1} + 12a_{n-2}, \text{ for } n \geq 2.$$

The first thing to do is to ignore the initial conditions and concentrate on the recurrence relation. And the way to solve the recurrence relation is to guess the solution. Actually it is to guess the **form** of the solution - an *educated* guess! For such a recurrence you should guess that the solution looks like $a_n = r^n$, for some constant r . In other words, guess the solution is simply the powers of some fixed number. The good news is that this guess will always be correct! You will always find some solutions of this form. When this guess is plugged into the recurrence relation and the equation is simplified, the result is an equation that can be solved for r . That equation is called the **characteristic equation** for the recurrence. In our example, when $a_n = r^n$ for each n , the result is $r^n = 4r^{n-1} + 12r^{n-2}$, and canceling r^{n-2} from each term, and rearranging the equation, we get $r^2 - 4r - 12 = 0$. That's the characteristic equation. The left side can be factored, and the equation then looks like $(r - 6)(r + 2) = 0$, and we see the solutions for r are $r = 6$ and $r = -2$. Sure enough, if you check it out, you will see that $a_n = 6^n$ and $a_n = (-2)^n$ both satisfy the given recurrence relation. In other words, we find that

$$6^n = 4 \cdot 6^{n-1} + 12 \cdot 6^{n-2} \text{ and } (-2)^n = 4 \cdot (-2)^{n-1} + 12 \cdot (-2)^{n-2}, \text{ for all } n \geq 2.$$

Using the characteristic equation, we have a method of finding some solutions to a recurrence relation. This method will not find all possible solutions. *BUT* if we find **all** the solutions to the characteristic equation, then they can be combined in a certain way to produce all possible solutions to the recurrence relation. The fact to remember is that if $r = a, b$ are the two solutions to the characteristic equation (for a recurrence of order two), then every possible solution to the linear homogeneous recurrence relation must look like $\alpha a^n + \beta b^n$ for some constants α, β .

In the example we have been working on every solution looks like $a_n = \alpha \cdot 6^n + \beta \cdot (-2)^n$. This expression is called the **general solution** of the recurrence relation.

Once we have figured out the general solution to the recurrence relation, it is time to think about the initial conditions. In our case, the initial conditions are $a_0 = 4$ and $a_1 = 8$. The idea is to select the constants α and β of the general solution $a_n = \alpha \cdot 6^n + \beta \cdot (-2)^n$ so it will produce the correct two initial values. For $n = 0$ we see we need $4 = a_0 = \alpha \cdot 6^0 + \beta \cdot (-2)^0 = \alpha + \beta$, and for $n = 1$, we need $8 = a_1 = \alpha \cdot 6^1 + \beta \cdot (-2)^1 = 6\alpha - 2\beta$. Now, we solve the following pair of linear equations for α and β :

$$\alpha + \beta = 4$$

$$6\alpha - 2\beta = 8.$$

By any technique for solving a system of two linear equations in two unknowns from basic algebra we find $\alpha = \beta = 2$. So, the solution is $a_n = 2 \cdot 6^n + 2 \cdot (-2)^n, n \geq 0$.

The steps in solving a degree k linear recurrence relation with constant coefficients are:

- (1) Determine the characteristic equation $\chi(x)$.
- (2) Find the solutions $r_1, r_2, \dots, r_k$ to $\chi(x) = 0$ (these are called the characteristic roots).
- (3) Write down the general solution $a_n = \alpha r_1^n + \beta r_2^n + \dots + \zeta r_k^n$.
- (4) Solve a system of two linear equations to find the constants $\alpha, \beta, \dots, \zeta$ that produce the correct initial conditions.

One catch with the method of characteristic equation occurs when the equation has repeated roots. Suppose that when the characteristic equation factors as $(r - 2)(r - 2)(r - 3)(r + 5)$. The characteristic roots are 2, 2, 3 and -5. Here 2 is a repeated root. If we follow the instructions given above, then the general solution we would write down is

Equation 36.1

$$a_n = \alpha 2^n + \beta 2^n + \gamma 3^n + \delta (-5)^n.$$

However, this expression will **not** include all possible solutions to the recurrence relation. Happily, the problem is not too hard to repair: each time a root of the characteristic equation is repeated, multiply it by an additional factor of n in the general solution, and then proceed as before.

For our example, we modify one of the 2^n terms in equation [36.1](#). The correct general solution looks like

$$a_n = \alpha 2^n + \beta n 2^n + \gamma 3^n + \delta (-5)^n.$$

Notice the extra factor of n in the second term. If $(r - 2)$ had been a four-fold factor of the characteristic equation, in other words, if 2 had been a characteristic root four times, then the part of the general solution involving the 2's would look like

$$\alpha 2^n + \beta n \cdot 2^n + \gamma n^2 \cdot 2^n + \delta n^3 \cdot 2^n.$$

Each new occurrence of a 2 is multiplied by one more factor of n .

Formally, the **characteristic equation** of the recursive formula $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$ is $\chi(x) = x^k - c_1 x^{k-1} - \dots - c_{k-1} x - c_k$. Notice that the degree of $\chi(x)$ coincides with the degree of the recurrence relation. Notice also that the non-leading coefficients of $\chi(x)$ are simply the negatives of the coefficients of the recurrence relation.

A number r (possibly complex) is a **characteristic root** if $\chi(r) = 0$. From basic algebra we know that r is a root of a polynomial if and only if $(x - r)$ is a factor of the polynomial. When $\chi(x)$ is a degree 2 polynomial, by the quadratic formula, either $\chi(x) = (x - r_1)(x - r_2)$, where $r_1 \neq r_2$, or $\chi(x) = (x - r)^2$, for some r . So there are two theorems about degree 2 linear recurrence relations with constant coefficients.

Theorem 36.1. *Let c_1 and $c_2 \neq 0$ be real numbers. Suppose that the polynomial $x^2 - c_1 x - c_2$ has two distinct roots r_1 and r_2 . Then a sequence $a: \mathbb{N} \rightarrow \mathbb{R}$ satisfies the recursive formula*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}, \text{ for } n \geq 2$$

if and only if $a_m = \alpha r_1^m + \beta r_2^m$, for all $m \geq 0$, for some constants α and β .

Proof. If $a_m = \alpha r_1^m + \beta r_2^m$ for all $m \geq 0$, where α and β are some constants, then since

$$r_i^2 - c_1 r_i - c_2 = 0, \text{ for } i = 1, 2, \text{ we have } r_i^2 = c_1 r_i + c_2, \text{ for } i = 1, 2.$$

Thus, for $n \geq 2$

$$\begin{aligned} c_1 a_{n-1} + c_2 a_{n-2} &= c_1 (\alpha r_1^{n-1} + \beta r_2^{n-1}) + c_2 (\alpha r_1^{n-2} + \beta r_2^{n-2}) \\ &= \alpha r_1^{n-2} (c_1 r_1 + c_2) + \beta r_2^{n-2} (c_1 r_2 + c_2) \text{ distributing and combining} \\ &= \alpha r_1^{n-2} \cdot r_1^2 + \beta r_2^{n-2} \cdot r_2^2, \text{ by the remark above.} \\ &= \alpha r_1^n + \beta r_2^n = a_n \end{aligned}$$

Conversely, if the terms of a satisfy the recursive formula and have initial terms a_0 and a_1 , then one checks that the sequence $a_m = \alpha r_1^m + \beta r_2^m$ for $m \geq 0$ with

$$\alpha = \frac{a_1 - a_0 r_2}{r_1 - r_2} \text{ and } \beta = \frac{a_0 r_1 - a_1}{r_1 - r_2}$$

also satisfies the recursive formula and has the same initial conditions. The equations for α and β come from solving the system of linear equations

$$a_0 = \alpha(r_1)^0 + \beta(r_2)^0 = \alpha + \beta \text{ and } a_1 = \alpha(r_1)^1 + \beta(r_2)^1 = \alpha r_1 + \beta r_2. \blacksquare$$

Example 36.2. Solve the recurrence relation $a_0 = 2, a_1 = 3$ and $a_n = a_{n-2}$, for $n \geq 2$.

Solution. The recurrence relation is a linear homogeneous recurrence relation of degree 2 with constant coefficients $c_1 = 0$ and $c_2 = 1$. The characteristic polynomial is

$$\chi(x) = x^2 - 0 \cdot x - 1 \cdot 1 = x^2 - 1.$$

The characteristic polynomial has two distinct roots since

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

Let us say that $r_1 = 1$ and $r_2 = -1$. Then the system of equations for $a_0 = 2, a_1 = 3$ are:

$$2 = a_0 = \alpha \cdot 1^0 + \beta(-1)^0 = \alpha + \beta$$

$$3 = a_1 = \alpha \cdot 1^1 + \beta(-1)^1 = \alpha - \beta$$

We can eliminate β by adding the equations together: $5 = 2\alpha$. Thus $\alpha = 5/2$. Substituting this back into the equation $\alpha + \beta = 2$ gives that $\beta = -1/2$. So our solution is

$$a_n = \frac{5}{2} \cdot 1^n - \frac{1}{2}(-1)^n = \frac{1}{2}(5 - (-1)^n) \text{ for } n \geq 0.$$

Example 36.3. Solve the recurrence relation $a_1 = 3, a_2 = 5, a_n = 5a_{n-1} - 6a_{n-2}$, for $n \geq 2$.

Solution. The characteristic polynomial is

$$\chi(x) = x^2 - 5 \cdot x + 6 = (x - 2)(x - 3).$$

The characteristic polynomial has two distinct roots $r_1 = 2$ and $r_2 = 3$. Then the system of equations for $a_1 = 3, a_2 = 5$ are:

$$3 = a_1 = \alpha \cdot 2^1 + \beta 3^1 = 2\alpha + 3\beta$$

$$5 = a_2 = \alpha \cdot 2^2 + \beta 3^2 = 4\alpha + 9\beta$$

We can eliminate α by multiplying the top equation by 2 and then subtracting the second equation from the first: $1 = -3\beta$. Thus $\beta = -1/3$. Substitute this back into $2\alpha + 3\beta = 3$ to get that $\alpha = 2$. So, our solution is

$$a_m = 2 \cdot 2^m - \frac{1}{3}3^m = 2^{m+1} - 3^{m-1} \text{ for } m \geq 1.$$

In case a characteristic polynomial of degree two has one repeated root we provide the theorem without proof.

Theorem 36.4. Let c_1 and c_2 be real numbers with $c_2 \neq 0$ and suppose also that the polynomial $x^2 - c_1x - c_2$ has a root r with multiplicity 2, so that $x^2 - c_1x - c_2 = (x - r)^2$. Then a sequence $a: \mathbb{N} \rightarrow \mathbb{R}$ satisfies the recursive formula

$$a_n = c_1a_{n-1} + c_2a_{n-2}, \text{ for } n \geq 2$$

if and only if $a_m = \alpha r^m + \beta m r^m$, for all $m \geq 0$, for some constants α and β .

Example 36.5. Solve the recurrence relation $a_0 = -1, a_1 = 4$ and $a_n = 4a_{n-1} - 4a_{n-2}$, for indices $n \geq 2$.

Solution. The characteristic polynomial is

$$\chi(x) = x^2 - 4 \cdot x + 4 = (x - 2)^2.$$

The general solution is now $a_m = (\alpha + \beta m)2^m$ aka $a_m = \alpha 2^m + \beta m 2^m$. The system of equations for $a_0 = -1, a_1 = 4$ are:

$$-1 = a_0 = \alpha \cdot 2^0 + \beta \cdot 0 \cdot 2^0 = \alpha$$

$$4 = a_1 = \alpha \cdot 2^1 + \beta \cdot 1 \cdot 2^2 = 2\alpha + 4\beta$$

Substitute $\alpha = -1$ into $2\alpha + 4\beta = 4$ to get that $\beta = 3$. So, our solution is

$$a_m = (-1) \cdot 2^m + 3m \cdot 2^m = (3m - 1)2^m \text{ for } m \geq 0.$$

Finally, we state, without proof, the general method of characteristic roots.

Theorem 36.6. Let $c_1, c_2, \dots, c_k \in \mathbb{R}$ with $c_k \neq 0$. Suppose that

$$\chi(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_{k-1} x - c_k = (x - r_1)^{j_1} (x - r_2)^{j_2} \cdot \dots \cdot (x - r_s)^{j_s}$$

where $r_1, r_2, \dots, r_s$ are distinct roots of $\chi(x)$, and $j_1, j_2, \dots, j_s$ are positive integers so that

$$j_1 + j_2 + j_3 + \dots + j_s = k.$$

Then a sequence $a: \mathbb{N} \rightarrow \mathbb{R}$ satisfies the recursive formula

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}, \text{ for } n \geq k$$

if and only if $a_m = p_1(m)r_1^m + p_2(m)r_2^m + \dots + p_s(m)r_s^m$ for $m \geq 0$, where

$$p_i(m) = \alpha_{0,i} + \alpha_{1,i}m + \alpha_{2,i}m^2 + \dots + \alpha_{j_i-1,i}m^{j_i-1}, \text{ for } 1 \leq i \leq s$$

and the $\alpha_{j,i}$'s are constants.

There is a problem with the general case. It is true that given the recurrence relation we can simply write down the characteristic polynomial. However, it can be quite a challenge to factor it as required by the theorem. Even if we succeed in factoring it, we are faced with the tedious task of setting up and solving a system of k linear equations in k unknowns (the $\alpha_{l,i}$'s). While in theory such a system can be solved using the methods of elimination or substitution covered in a college algebra course, in practice, the amount of labor involved can become overwhelming. For this reason, computer algebra systems are often used in practice to help solve systems of equations, or even the original recurrence relation.

Exercises

Exercise 36.1. For each of the following sequences find a recurrence relation satisfied by the sequence. Include a sufficient number of initial conditions to completely specify the sequence.

- (a) $a_n = 2n + 3, n \geq 0$.
- (b) $a_n = 3 \cdot 2^n, n \geq 1$.
- (c) $a_n = n^2, n \geq 1$.
- (d) $a_n = n + (-1)^n, n \geq 0$.

Solve each of the following recurrence relations:

Exercise 36.2. $a_0 = 3, a_1 = 6$ and $a_n = a_{n-1} + 6a_{n-2}$, for $n \geq 2$.

Exercise 36.3. $a_0 = 4, a_1 = 7$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$.

Exercise 36.4. $a_2 = 5, a_3 = 13$ and $a_n = 7a_{n-1} - 10a_{n-2}$ for $n \geq 4$.

Exercise 36.5. $a_1 = 3, a_2 = 5$ and $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 3$.

Exercise 36.6. $a_0 = 1, a_1 = 6$ and $a_n = 6a_{n-1} - 9a_{n-2}$ for $n \geq 2$.

Exercise 36.7. $a_1 = 2, a_2 = 8$ and $a_n = a_{n-2}$ for $n \geq 3$.

Exercise 36.8. $a_0 = 2, a_1 = 5, a_2 = 15$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ for $n \geq 3$.

Exercise 36.9. Find a closed form for the terms of the Fibonacci sequence: $f_0 = 0, f_1 = 1$, and for $n \geq 2, f_n = f_{n-1} + f_{n-2}$.

Problems

Solve each of the recurrence relations using the method of characteristic roots:

Problem 36.1. $a_0 = 1$ and $a_n = 2a_{n-1}$ for $n \geq 1$.

Problem 36.2. $a_0 = 2, a_1 = 5$ and $a_n = a_{n-1} + 6a_{n-2}$ for $n \geq 2$.

Problem 36.3. $a_0 = 3, a_1 = 7$ and $a_n = 6a_{n-1} - 5a_{n-2}$ for $n \geq 2$.

Problem 36.4. $a_2 = 5, a_3 = 13$ and $a_n = 3a_{n-1} + 10a_{n-2}$ for $n \geq 4$.

Problem 36.5. $a_1 = 3, a_2 = 5$ and $a_n = 8a_{n-1} - 16a_{n-2}$ for $n \geq 3$.

Problem 36.6. $a_1 = 2, a_2 = 8$ and $a_n = 4a_{n-2}$ for $n \geq 3$.

Problem 36.7. $a_0 = 0, a_1 = 1, a_2 = 2$ and $a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3}$ for $n \geq 3$.

Problem 36.8. $a_0 = 0, a_1 = 1$ and for $n \geq 2, a_n = 2a_{n-1} + a_{n-2}$.

Chapter 37: Solving Non-homogeneous Recurrence Relations

When a linear recurrence relation with constant coefficients for a sequence $\{s_n\}$ looks like

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_k s_{n-k} + f(n),$$

where $f(n)$ is some (nonzero) function of n , then the recurrence relation is said to be **non-homogeneous**. For example, $s_n = 2s_{n-1} + n^2 + 1$ is a non-homogeneous recurrence. In this case $f(n) = n^2 + 1$. The methods used in the last chapter are not adequate to deal with non-homogeneous problems. But it wasn't all a waste since those methods do provide one step in the solution of non-homogeneous problems.

The steps used to solve non-homogeneous linear recurrence relations with constant coefficients are:

- (1) Replace the function $f(n)$ with 0 to create the associated homogeneous recurrence

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_k s_{n-k}.$$

Find the characteristic roots and write down the general solution. We learned to do this in chapter 36. For example, if $\chi(x) = x^k - c_1 x^{k-1} - \cdots - c_{k-1} x - c_k$ has no repeated roots, the general solution will be $s_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$ where the constants α_i are to be determined.

- (2) Find one **particular solution** to the original non-homogeneous recurrence relation. That is, find a specific sequence that obeys the recursive equation ignoring the initial conditions. The correct procedure here is to guess. You will want your guess to be an educated one. An educated guess will depend on the form of $f(n)$. There is a complicated algorithm for making the correct guess, but it isn't worth learning for the small number of examples we will be doing. Instead we will rely on the following guidelines to inform our guess. The plan is to guess a particular solution that is the most general function of the same type as $f(n)$. Table 37.1 shows reasonable guesses.

$f(n)$	Particular Solution Guess
c (a constant)	A (a constant)
n	$An + B$
n^2	$An^2 + Bn + C$
n^3	$An^3 + Bn^2 + Cn + D$
2^n	$A \cdot 2^n$
r^n (r constant)	$A \cdot r^n$

Table 37.1: Particular Solution Patterns

These guesses can be *mixed-and-matched*. For example, if $f(n) = 3n^2 + 5^n$ then a good candidate for a particular solution would be $An^2 + Bn + C + D \cdot 5^n$.

Once a guess has been made for the form of a particular solution, that guess is plugged into the recurrence relation, and the coefficients $A, B, \dots$ are determined. In this way a specific particular solution will be found.

It will sometimes happen that when the equations are set up to determine the coefficients of the particular solution an inconsistent system will appear. In such a case, as with repeated characteristic roots, the trick is (more-or-less) to multiply the guess for the particular solution by n and try again.

- (3) Once a particular solution has been found, add the particular solution to the general solution of the homogeneous recurrence relation from step (1). If we denote the particular solution by $h(n)$, then the total general solution looks like

$$s_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \dots + \alpha_k r_k^n + h(n).$$

- (4) Invoke the initial conditions to determine the values of the coefficients $\alpha_1, \dots, \alpha_k$ exactly as was done in chapter 36.

The major oversight made in solving a non-homogeneous recurrence relation is trying to determine the coefficients $a_1, a_2, \dots, a_k$ before the particular solution is added to the general solution. This mistake will usually lead to inconsistent information about the coefficients, and no solution to the recurrence will be found.

Example 37.1. *Let's solve the Tower of Hanoi recurrence using this method. The recurrence is $H_0 = 0$, and, for $n \geq 1$, $H_n = 2H_{n-1} + 1$. We know the closed form formula for H_n is $2^n - 1$ for $n \geq 0$ already, but let's work it out using the method outlined above.*

- (1) The associated homogeneous recurrence is $H_n^{(h)} = 2H_{n-1}^{(h)}$. The characteristic root is 2. The general solution will be $H_n^{(h)} = \alpha \cdot 2^n$ where the constant α is to be determined.
- (2) Based on Table 37.1 we will guess the particular solution (indicated by a superscript (p)) as $H_n^{(p)} = A$ for some constant A . When we substitute A for each term H_k in the relation we arrive at $A = 2A + 1$. Thus $A = -1$.
- (3) Thus, the general solution for the Tower of Hanoi recurrence is

$$H_n = H_n^{(h)} + H_n^{(p)} = \alpha \cdot 2^n - 1.$$

- (4) The initial condition $H_0 = 0$ gives $0 = H_0 = \alpha \cdot 2^0 - 1 = \alpha - 1$. Thus $\alpha = 1$. So, the final solution of the Tower of Hanoi recurrence is $H_n = 2^n - 1$ for $n \geq 0$ as we found before.

Example 37.2. *Here is a more complicated example worked out in detail to exhibit the method. Let's solve $s_1 = 2, s_2 = 5$ and $s_n = s_{n-1} + 6s_{n-2} + 3n - 1$ for $n \geq 3$.*

- (1) The associated homogeneous recurrence is $s_n^{(h)} = s_{n-1}^{(h)} + 6s_{n-2}^{(h)}$. The characteristic polynomial is $x^2 - x - 6 = (x - 3)(x + 2)$. The characteristic roots are 3, -2. The

general solution will be $s_n^{(h)} = \alpha \cdot 3^n + \beta \cdot (-2)^n$ where the constants α, β are to be determined.

- (2) Based on Table 37.1 we will guess the particular solution $s_n^{(p)} = An + B$ for some constants A, B . When we substitute $Ak + B$ for each term s_k in the relation we arrive at

$$An + B = A(n - 1) + B + 6[A(n - 2) + B] + 3n - 1.$$

Collect the linear terms and constant terms:

$$(6A + 3)n + (-13A + 6B - 1) = 0.$$

If this is correct for all values of n , then $6A + 3 = 0$ and $-13A + 6B = 1$. So by basic algebra we find $A = -1/2$ and $B = -11/12$.

- (3) Thus, the general solution for this recurrence is

$$s_n = \alpha \cdot 3^n + \beta(-2)^n - \frac{1}{2}n - \frac{11}{12}.$$

- (4) The initial conditions $s_1 = 2$ and $s_2 = 5$ give the equations

$$2 = 3\alpha - 2\beta - \frac{1}{2} - \frac{11}{12}$$

$$5 = 9\alpha + 4\beta - 1 - \frac{11}{12}.$$

Solve this system of two linear equations in two unknowns: $\alpha = 11/12$ and $\beta = -1/3$.

So, the final solution of the recurrence is $s_n = \frac{11}{12} \cdot 3^n - \frac{1}{3} \cdot (-2)^n - \frac{1}{2}n - \frac{11}{12}$ for $n \geq 0$.

Exercises

Use the general solutions for the related homogeneous problems of chapter [36](#) to help solve the following non-homogeneous recurrence relations with initial conditions.

Exercise 37.1. $a_0 = 3, a_1 = 6$ and $a_n = a_{n-1} + 6a_{n-2} + 1$ for $n \geq 2$.

Exercise 37.2. $a_2 = 5, a_3 = 13$ and $a_n = 7a_{n-1} - 10a_{n-2} + n$ for $n \geq 4$.

Exercise 37.3. $a_1 = 3, a_2 = 5$ and $a_n = 4a_{n-1} - 4a_{n-2} + 2^n$ for $n \geq 3$.

Exercise 37.4. $a_0 = 1, a_1 = 6$ and $a_n = 6a_{n-1} - 9a_{n-2} + n$ for $n \geq 2$.

Exercise 37.5. $a_0 = 2, a_1 = 5$ and $a_2 = 15$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3} + 2n + 1$ for $n \geq 3$.

Problems

Solve the following non-homogeneous recurrence relations with initial conditions.

Problem 37.1. $a_0 = 1$ and $a_n = 2a_{n-1} + 1$ for $n \geq 1$.

Problem 37.2. $a_0 = 2, a_1 = 5$ and $a_n = a_{n-1} + 6a_{n-2} + 2$ for $n \geq 2$.

Problem 37.3. $a_0 = 3, a_1 = 7$ and $a_n = 6a_{n-1} - 5a_{n-2} + n$ for $n \geq 2$.

Problem 37.4. $a_2 = 5, a_3 = 13$ and $a_n = 3a_{n-1} + 10a_{n-2} + n + 2$ for $n \geq 4$.

Problem 37.5. $a_1 = 3, a_2 = 5$ and $a_n = 8a_{n-1} - 16a_{n-2} + n^2$ for $n \geq 3$.

Problem 37.6. $a_1 = 2, a_2 = 8$, and $a_n = 4a_{n-2} + 2^n$ for $n \geq 3$.

Problem 37.7. $a_0 = 0, a_1 = 1, a_2 = 2$ and $a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3} + 2n$ for $n \geq 3$.

Problem 37.8. $a_0 = 0, a_1 = 1$, and for $n \geq 2$, $a_n = 2a_{n-1} + a_{n-2} + 1$.

PART VI: Graph Theory

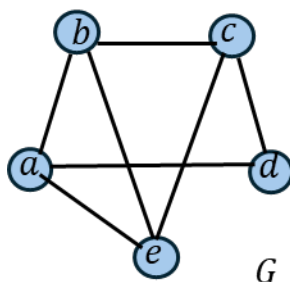
Chapter 38: Graph Isomorphism

In chapter [8](#) we represented a relation with a graph. In this chapter we discuss a more general notion of a graph.

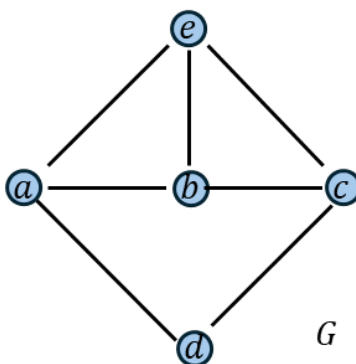
In this chapter, a **graph** will consist of a set of points (called **vertices**) (singular: **vertex**) together with a set of lines (called **edges**) joining some (possibly none, possibly all) pairs of vertices. When we allow loops, multiple edges between vertices or directed edges we will explicitly make that clear. Otherwise, in this chapter the graphs will be **simple** meaning no loops, multiple connections between two vertices and no directions on the edges. All graphs will have finite vertex sets, and consequently a finite number of edges. Graphs are typically denoted by an uppercase letter such as G or H .

Formally a (simple) **graph** G consists of a set of vertices V and a set E of edges. An edge $t \in E$ is written as an unordered pair of vertices $\{u, v\}$ – meaning two different vertices. The edge denoted $t = \{u, v\}$ has **endpoints** u and v . We say the edge t is **incident** with both u and v . The vertices u and v are **adjacent** when there is an edge with endpoints u and v . When $\{u, v\}$ is not an edge u and v are not adjacent. Often the most useful way to think of a graph is as a diagram.

Here is an example of a graph G with vertex set $\{a, b, c, d, e\}$ illustrating these concepts.



The placement of the vertices in a diagram representing a graph is (within reason!) not important. Here is another diagram of that same graph G .



In both diagrams for the graph G we have vertex set $\{a, b, c, d, e\}$ and edges $\{a, b\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, e\}, \{c, d\}$ and $\{c, e\}$. That is all that matters – that a diagram for a graph correctly represents the vertex set and the adjacency of vertices using edges.

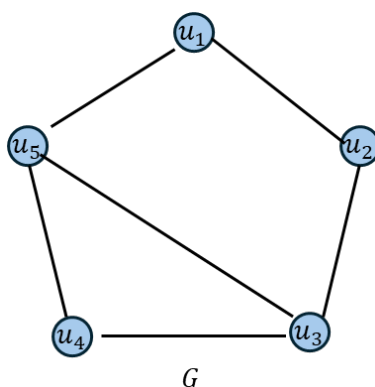
We do try to use straight line edges as opposed to curved edges. For clarity we mark vertices to clearly distinguish them from locations where edges overlap. When possible we avoid edges that cross.

There are two standard ways to represent a graph in computer memory. Both methods use the so-called 0,1 –matrices as used in Chapter 8.

If a (simple) graph G has n vertices an **adjacency matrix** for G is an $n \times n$ matrix with both rows and columns labeled by vertices so that the entry in the row labeled x and column labeled y is 1 if $\{x, y\}$ is an edge and 0 otherwise. We will use the same ordering of vertices for both rows and columns – for similar reasons as in Chapter 8. Notice the article preceding adjacency matrix is indefinite. This is because any ordering of the vertex set will give rise to a valid matrix.

An **incidence matrix** for a (simple) graph G with n vertices and m edges is an $n \times m$ 0,1 –matrix whose rows are labeled by the vertices and columns labeled by the edges so that the entry labeled by the vertex x and edge e is 1 if x and e are incident and 0 otherwise.

Example 38.1. Let G have edges $\{u_1, u_2\}, \{u_2, u_3\}, \{u_3, u_4\}, \{u_4, u_5\}, \{u_5, u_1\}, \{u_5, u_3\}$ and vertices $\{u_1, u_2, u_3, u_4, u_5\}$. A graphical presentation of G is



Here are the adjacency matrix A_G and the incidence matrix M_G using the ordering of edges and vertices as given.

$$A_G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}, \quad M_G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

You might guess that we will prefer adjacency matrices since they will usually be more efficient in representing the graph.

Unlike most areas of mathematics, it is possible to point to a specific person as the creator of graph theory and a specific problem that led to its creation. The problem is called the *Seven Bridges of Königsberg* problem. Leonhard Euler used a graph theoretic approach to exhibit a solution in 1736. The citizens of Königsberg would attempt to cross every bridge in town without retracing steps and finish where they started. Euler demonstrated that this could not be done – and ruined their weekend pastime. More on this problem in the next chapter.

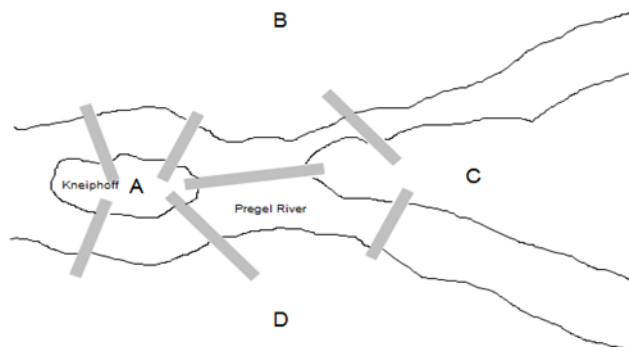


Figure 38.1: The Seven Bridges of Königsberg

The notion of a graph is a little more general than the simple case we are considering. For example, **multigraphs** allow multiple edges between pairs of vertices (think of airline flights connecting two cities). **Pseudographs** allow loops at vertices. Directed graphs, aka **digraphs**, impose an ordering on each edge.

For a vertex v in a graph G let us denote the number of edges incident with v as the **degree** of v , written as $\deg v$. Consider the graph of Example 38.1. The vertices u_1, u_2 and u_4 each have degree 2 while $\deg u_3 = \deg u_5 = 3$. The list of degrees of the vertices of a graph is called the **degree sequence** of the graph. It is customary to list the degrees in increasing order. Thus, the degree sequence for the graph from Example 38.1 is 2,2,2,3,3 or more succinctly $2^3, 3^2$.

Theorem 38.2. *The sum of the degrees of the vertices of an (undirected) graph equals twice the number of edges. Thus, the sum of degrees is even.*

Proof. When adding the degrees for the vertices each edge contributes exactly two to the total. ■

Referring to the graph from Example 38.1 the sum of the degrees of vertices is

$$2 + 2 + 2 + 3 + 3 = 12 = 2 \cdot 6.$$

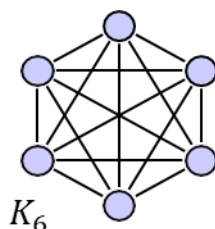
Corollary 38.3. *A graph must have an even number of vertices of odd degree.*

Proof. Split the vertices into two subsets – those with even degree and those with odd degree. The sum of all degrees is even. The sum of degrees of vertices with even degree is also even. Thus the sum of the degrees of vertices with odd degree must be even. There must therefore be an even number of odd numbers in the sum. ■

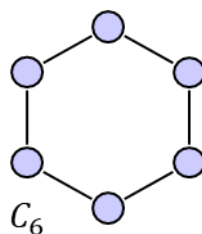
Corollary 38.4. *In a directed graph the sum of the degrees into vertices must equal to the sum of the degrees out of vertices.*

We next display several families of commonly occurring graphs.

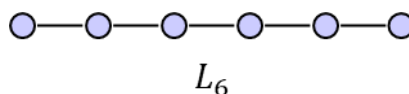
For $n \geq 0$, K_n denotes the (simple) graph with n vertices where every pair of vertices is adjacent. The graph K_n is called the **complete graph** on n vertices. It is maximal among all simple graphs on n vertices with respect to the number of edges in the graph.



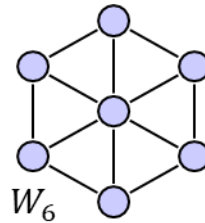
For $n \geq 3$, C_n denotes the graph with vertices $v_1, v_2, \dots, v_n$ with adjacency determined by $\{v_i, v_j\}$ is an edge if and only if $j \equiv i + 1 \pmod{n}$. That is v_i is adjacent to v_{i+1} for $i = 1, \dots, n - 1$ and v_n is adjacent to v_1 . The graph C_n is called an **n – cycle**.



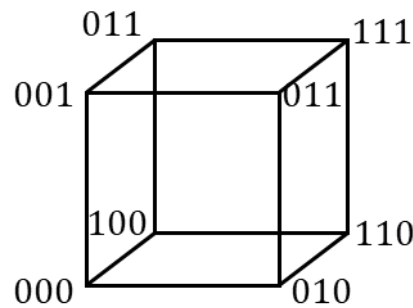
For $n \geq 0$, L_n denotes the graph with vertices $v_1, v_2, \dots, v_n$ with adjacency determined by v_i is adjacent to v_{i+1} for $i = 1, \dots, n - 1$. Alternately, for $n \geq 3$, the graph L_n is produce when an edge of C_n is removed. The graph L_n is called the **n – link**.



For $n \geq 3$, W_n denotes the **n –wheel**. The n –wheel is formed by adding a central hub vertex to the n –cycle C_n . The n –wheel will therefore have $n + 1$ vertices.

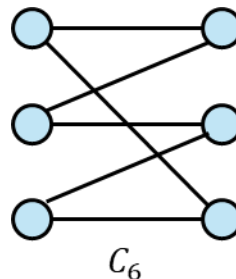


For $n \geq 0$, the **n –cube**, Q_n , is the graph whose vertices are labeled with the 2^n bit strings of length n . Two vertices are adjacent provided that the underlying bit strings differ in exactly one position. For $n > 4$ representing the graph visually and esthetically is notoriously hard.



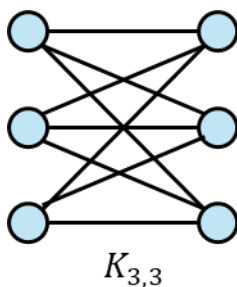
An important class of graphs that we've utilized before are called **bipartite** graphs. A graph G is bipartite if its vertex set $V = V_1 \cup V_2$ with $V_1 \cap V_2 = \emptyset$ and $V_1 \neq \emptyset \neq V_2$ and all edges of the graph are of the form $\{a, b\}$ where $a \in V_1$ and $b \in V_2$. Such a graph can be drawn using the set of vertices V_1 (standardly on the left) and V_2 where there are no edges among vertices in either V_1 or V_2 .

As an example, the graph C_6 can be drawn as follows:



If $|V_1| = m \geq 1$, $|V_2| = n \geq 1$ and every vertex of V_1 is adjacent to every vertex of V_2 the graph is denoted $K_{m,n}$ and called a **complete bipartite** graph.

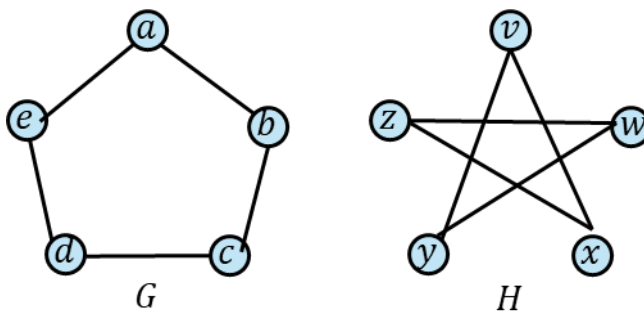
Here is the graph $K_{3,3}$:



It is not always obvious that a graph is bipartite, but we describe an algorithm that will help to decide. Pick two colors (red and blue will do). Color any vertex in the graph red. Color all of its adjacent vertices (neighbors) blue. Color the neighbors of each blue vertex red and so on. You will either wind up with a consistent coloring where no red vertex is adjacent to another and similarly for blue. Meaning all edges are incident with one red vertex and one blue vertex. Use the red colored vertices as V_1 and the blue colored vertices as V_2 . If your coloring is not consistent (meaning two red neighbors or two blue neighbors) the graph is not bipartite.

The notion of sameness for graphs – meaning that one can be redrawn to be identical to the other is important. If G can be redrawn so as to be the same as H we say that G and H are **isomorphic** and we write $G \cong H$. This redrawing requires a map φ from the vertices of G to the vertices of H which must be bijective if there is any hope of the graphs representing the same object. But more than that the map must have the **adjacency-preserving** property that $\{u, v\}$ is an edge of G if and only if $\{\varphi(u), \varphi(v)\}$ is an edge in H . This means that after re-ordering the vertices of H the adjacency matrix for G using ordering $a, b, c, \dots$ is identical to the adjacency matrix A_H^φ for H using the ordering $\varphi(a), \varphi(b), \varphi(c), \dots$.

Example 38.5. Let G be the 5-cycle with vertices a, b, c, d, e and edges $\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, a\}$ drawn to resemble a regular convex pentagon. Let H be the graph shown with vertex set $\{v, w, x, y, z\}$ and edges $\{v, x\}, \{x, z\}, \{z, w\}, \{w, y\}, \{y, v\}$.



With respect to alphabetical ordering the adjacency matrices for G and H are as follows:

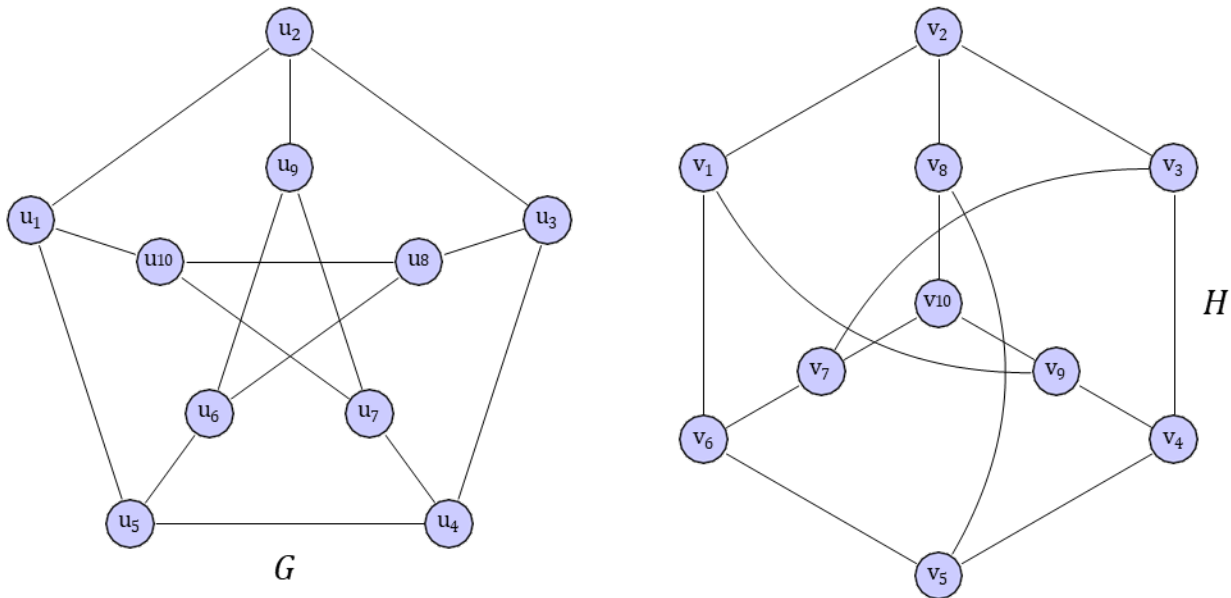
$$A_G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \neq A_H = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Let $\varphi = \{(a, v), (b, x), (c, z), (d, w), (e, y)\}$. Then φ has the adjacency-preserving property since when the vertices of H are ordered v, x, z, w, y we have

$$A_H^\varphi = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = A_G$$

The map φ is called a **graph isomorphism**.

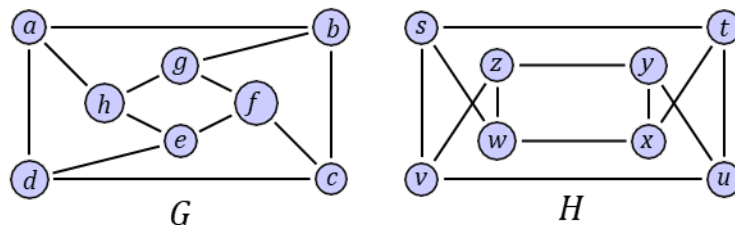
Example 38.6. The two graphs shown below are isomorphic since the map φ with ordered pairs $\{(u_1, v_1), (u_2, v_2), (u_3, v_3), (u_4, v_4), (u_5, v_9), (u_6, v_{10}), (u_7, v_5), (u_8, v_7), (u_9, v_8), (u_{10}, v_6)\}$ has the adjacency-preserving property. You should check this by finding A_G and A_H^φ .



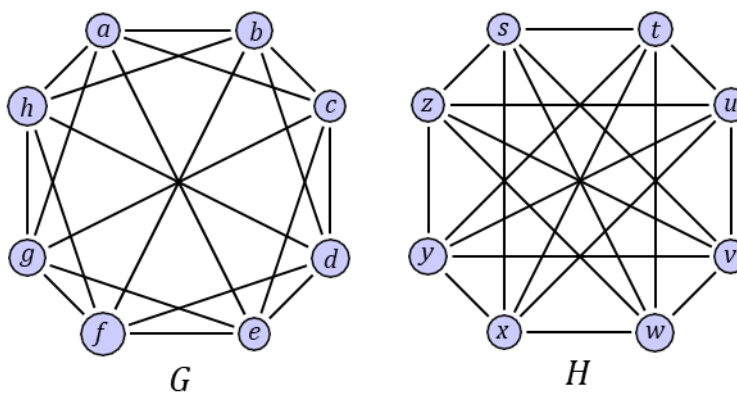
The graph G is the standard presentation of the **Petersen Graph**. It can be described as the graph whose vertex set is labeled by all 2 –subsets of a 5 –set and where an edge joins two vertices if the underlying 2 –sets are disjoint.

Exercises

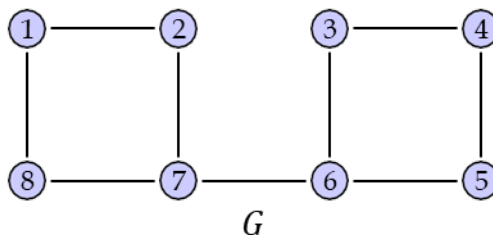
Exercise 38.1. Find a graph isomorphism $\varphi: G \rightarrow H$. Verify the adjacency-preserving property by showing that the adjacency matrices A_G and A_H^φ are identical.



Exercise 38.2. Prove that the graphs G and H are not isomorphic.



Exercise 38.3. Redraw the graph G as a bipartite graph.

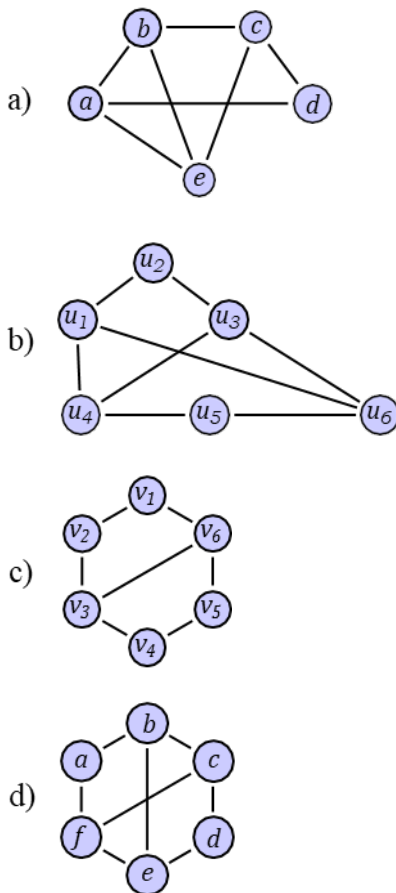


Problems

Problem 38.1. Answer the following questions:

- (a) How many edges are there in K_n the complete graph on n vertices?
- (b) How many edges are there in C_n the n –cycle on n vertices?
- (c) How many edges are there in L_n the n –link on n vertices?
- (d) How many edges are there in W_n the n –wheel on $n + 1$ vertices?
- (e) How many edges are there in Q_n the n –cube on 2^n vertices?
- (f) How many edges are there in $K_{m,n}$ the complete bipartite graph with m left vertices and n right vertices?

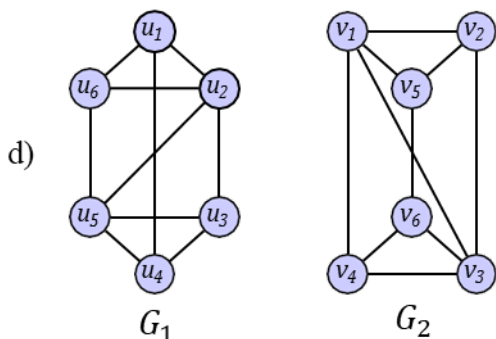
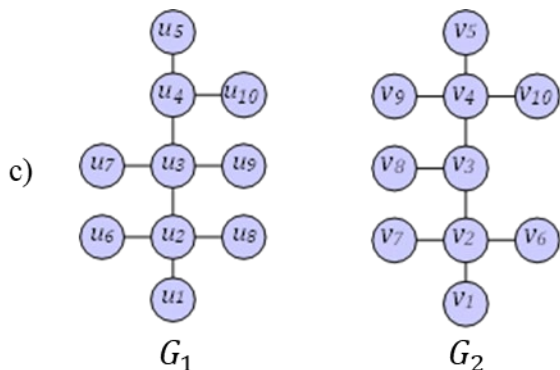
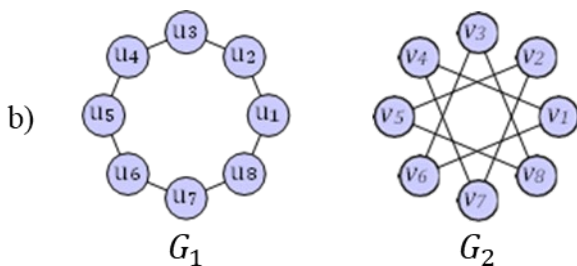
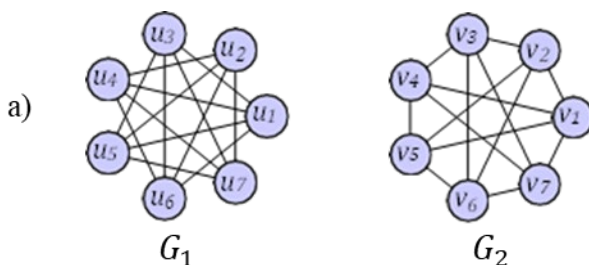
Problem 38.2. Determine whether each graph is bipartite. If it is, redraw it as a bipartite graph.



Problem 38.3. a) For which values of n is C_n bipartite? b) For which values of n is Q_n bipartite?

Problem 38.4. Draw the Petersen graph with vertices labeled with the 2 –subsets of $\{a, b, c, d, e\}$ and adjacency as suggested in example [38.5](#).

Problem 38.5. For each pair of graphs either prove that G_1 and G_2 are not isomorphic, or else show that they are isomorphic by exhibiting a graph isomorphism ψ . Validate that you have an isomorphism by showing that $A_{G_1} = A_{G_2}^\psi$ when vertices are ordered appropriately.



Problem 38.7. Prove theorem 38.7: If G is a connected graph, then there is a simple path between any two different vertices.

Chapter 39: Paths

The origins of graph theory had to do with bridges, and possible routes crossing the bridges. In this section we will consider that sort of question in graphs in general. We will think of walking along edges, from one vertex in the list to the next, and visiting vertices.

We begin with a collection of definitions. These terms are used differently in different texts. If you look at another graph theory text, be sure to see how the terms are used there.

A **path** of length n in a graph is an alternating sequence of vertices and edges of the form $v_0, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v_n$, where $e_i = \{v_{i-1}, v_i\}$, for $i = 1, 2, \dots, n$. A path is **simple** if no edge is repeated. A **circuit** is a path with $v_0 = v_n$. A simple circuit is a **cycle**. In a digraph we require $e_i = (v_{i-1}, v_i)$, for $i = 1, 2, \dots, n$. In a simple graph we can and will suppress the edges and therefore consider any string of pairwise incident vertices as a path. We will consider a single vertex v to be a path of length 0.

Here is an example illustrating these definitions.

Example 39.1. In the graph shown in figure 39.1, a, b, e, c, f, c is a path of length 5. That is an example of an a, c –path, meaning it starts at vertex a and ends at vertex c . That path is not simple since the edge c, f is repeated. Note that direction does not matter. The vertex sequence a, b, c, f, e is an a, e –path. Here are two simple circuits in the graph: a, b, e, d, a and a, b, c, e, d, a . Notice that the circuit a, e, b, c, f, e, d, a is also simple even though it repeats the vertex e . It does not repeat any edges.

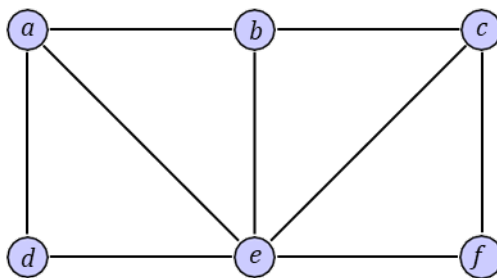


Figure 39.1: Examples of paths and circuits

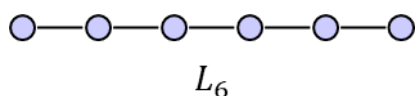
A graph is **connected** if there is a path between any two vertices. In plain English, a connected graph consists of a single piece. The individual connected pieces of a graph are called its **connected components**. The length of the shortest path between two vertices in a connected component of a graph is called the **distance** between the vertices. In figure 39.1, the distance between a and f is 2.

Theorem 38.7. In a connected graph there is a simple path between any two vertices. In other words, if there is a way to get from one vertex to another vertex along edges, then there is a way to get between those two vertices without repeating any edges.

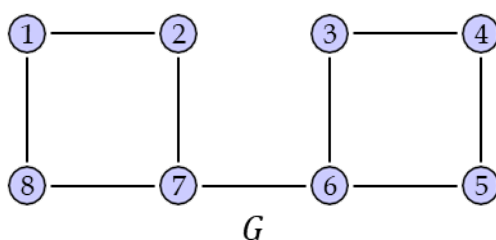
Proof. Exercise. The idea is simple: in a path with a repeated edge, just eliminate the side trip made between the two occurrences of that edge from the path. Do that until all the repeated edges are eliminated. ■

A vertex in a graph is a **cut-vertex**, if removal of the vertex and edges incident to it results in a graph with more connected components. Similarly, a **bridge** is an edge whose removal (keeping the vertices it is incident to) yields a graph with more connected components.

Example 39.2. In the 6 –link below the endpoints are not cut-vertices. But all of the internal vertices are cut-vertices.



Example 39.3. In the graph below the edge $\{6,7\}$ is a bridge. The graph G has no other edges that are bridges.



We close this section with a discussion of two special types of paths.

An **Eulerian path** in a graph is a simple path which transverses every edge of the graph. In other words, an Eulerian path in a graph is a path that transverses every edge of the graph exactly once. An interesting property of a graph with an Eulerian path is that it can be drawn completely without lifting pencil from paper and without retracing any edges.

An **Eulerian cycle** is a simple circuit in a graph that transverses every edge of the graph. So an Eulerian cycle is a path of length three or more that transverses every edge of the graph and ends up at its initial vertex. A graph is called **Eulerian** if it has either an Eulerian cycle or an Eulerian path.

Example 39.4. The graph C_5 is Eulerian. In fact, the graph itself is an Eulerian cycle.

Example 39.5. The graph K_5 is Eulerian. Start at any vertex. Trace the inner pentagon. Then trace the outer pentagon.

Example 39.6. The graph L_n is Eulerian. It does not have an Eulerian cycle.

Example 39.7. *The graph K_4 is not an Eulerian graph. Try it!*

A **Hamiltonian path** in a graph is a simple path that visits every vertex in the graph exactly once. A **Hamiltonian cycle** in a graph is a simple circuit that, except for the last vertex of the circuit, visits every vertex in the graph exactly once. A graph is **Hamiltonian** if it has a Hamiltonian cycle.

Example 39.8. K_n is Hamiltonian for $n \geq 3$.

Example 39.9. L_n has no Hamiltonian cycle for $n \geq 2$

A few easy observations: if G is a graph with either an Eulerian cycle or Hamiltonian cycle, then

1. G is connected.
2. Every vertex of G has degree at least 2.
3. G has no bridges.
4. If G has a Hamiltonian cycle, then G has no cutvertices.

Leonhard Euler gave a simple way to determine exactly when a graph is Eulerian. On the other hand, despite considerable effort, no one has been able to devise a test to distinguish between Hamiltonian and non-Hamiltonian graphs that is much better than a brute force trial-and-error search for a Hamiltonian circuit.

Theorem 39.10: *A connected multigraph has an Eulerian cycle if and only if every vertex has even degree.*

Proof. Let G be a connected multigraph with an Eulerian cycle and suppose that v is a vertex in G with $\deg(v) = 2m + 1$, for some $m \in \mathbb{N}$. Let i denote the number of times the cycle passes through v . Since every edge is used exactly once in the cycle, and each time v is visited 2 different edges are used, we have $2i = 2m + 1 \rightarrow \leftarrow$.

Conversely, let G be a connected multigraph where every vertex has even degree. Select a vertex u and build a simple path P starting at u . Each time a vertex is reached we add any edge not already used. Any time a vertex $v \neq u$ is reached its even degree guarantees a new edge out, since we used one edge to arrive there. Since G is finite, we must reach a vertex where P cannot continue. And this vertex must be u by the preceding remark. Therefore P is a cycle. If this cycle contains every edge we are done. Otherwise, when these edges are removed from G we obtain a set of connected components $H_1, \dots, H_m$. Each of these subgraphs satisfy the conditions of the theorem. Since their sizes are smaller, we may inductively construct an Eulerian cycle C_i for each H_i . Since G is connected each subgraph H_j contains a vertex, say v_j of the initial cycle. Now $v_0, \dots, v_j, C_j, v_j, \dots, v_n, v_0$ is a cycle in G . Since the H_j are disjoint we can insert all of the C_i 's. This results in an Eulerian cycle for G . ■

Corollary 39.11. *A connected multigraph has an Eulerian path, but no Eulerian cycle if and only if it has exactly two vertices of odd degree.*

The following theorem is an example of a sufficient condition for a graph to have a Hamiltonian cycle. It is attributed to Gabriel Andrew Dirac. This condition is clearly not necessary by considering C_n for $n \geq 5$. Any cycle has all vertices of degree 2 which is less than $n/2$ when $n \geq 5$.

Theorem 39.12. (Dirac) *Let G be a connected, simple graph on $n \geq 3$ vertices. If $\deg v \geq n/2$ for every vertex v , then G has a Hamiltonian cycle.*

Proof: Suppose that the theorem is false. Let G satisfy the conditions on vertex degree, connectivity, and simplicity. Moreover, suppose that of all counterexamples on n vertices, G is maximal with respect to the number of edges. G is not complete since K_n has a Hamiltonian cycle for all $n \geq 3$. Therefore G has two nonadjacent vertices v_1 and v_n .

By maximality the graph $G_1 = G \cup \{v_1, v_n\}$ has a Hamiltonian cycle. But also, this cycle uses the edge $\{v_1, v_n\}$ else the cycle is in G . So, we may suppose that the Hamiltonian cycle in G_1 is of the form $v_1, v_2, \dots, v_n, v_1$. Thus $v_1, \dots, v_n$ is a Hamiltonian path in G .

But let $k = \deg(v_1)$, i.e. $k = |S| = |\{v \in V \mid v \sim v_1\}|$. If $v_{i+1} \in S$, then $v_i \not\sim v_n$, else $v_1, \dots, v_i, v_n, v_{n-1}, \dots, v_{i+1}, v_1$ is a Hamiltonian cycle in G – see figure 39.2. Therefore $\deg(v_n) \leq n - 1 - k \leq n - 1 - \frac{n}{2} = \frac{n}{2} - 1 \rightarrow \leftarrow \blacksquare$

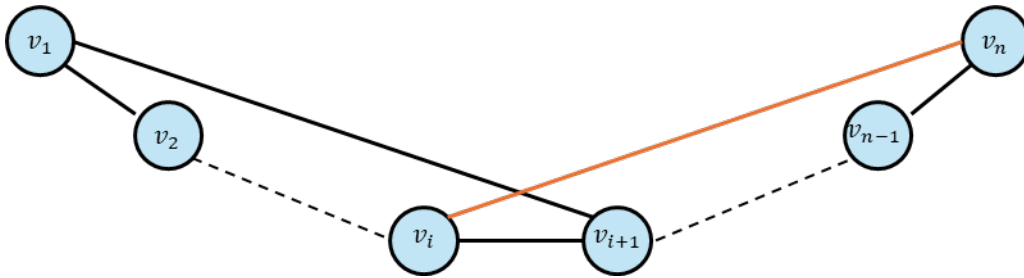
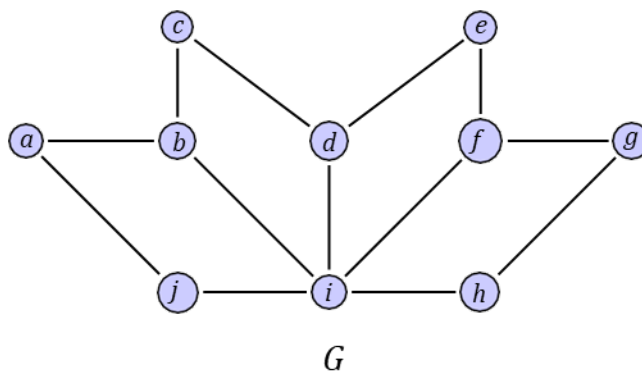


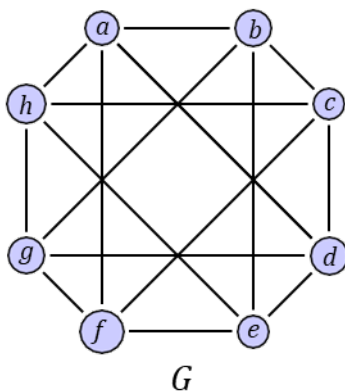
Figure 39.2: Graph for Dirac's Theorem

Exercises

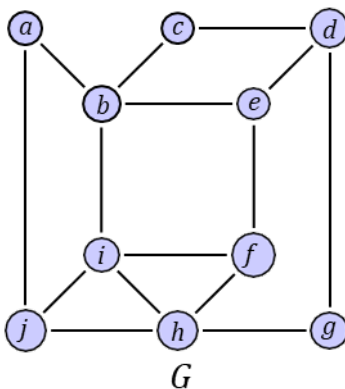
Exercise 39.1. Give a Hamiltonian cycle as a list of vertices for the graph G . Explain why G does not have an Eulerian cycle.



Exercise 39.2. Find an Eulerian cycle for the graph G as a list of vertices.



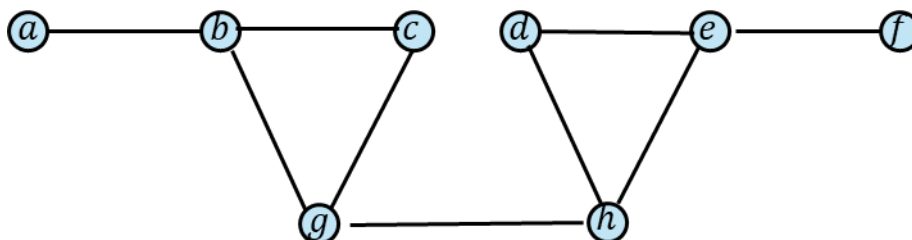
Exercise 39.3. Prove that the graph G has no Hamiltonian cycle.



Problems

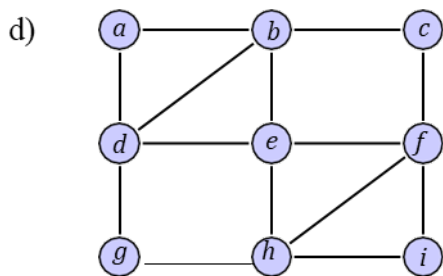
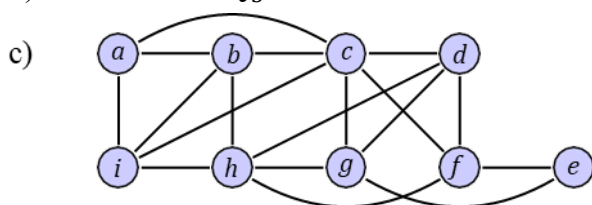
Problem 39.1. For the graph below

- (1) Find all bridges.
- (2) Find all cut-vertices.



Problem 39.2. For each graph below (i) find an Eulerian cycle as a list of vertices or prove that none exists and (ii) find a Hamiltonian cycle as a list of vertices or prove that none exists.

- a) The Petersen Graph.
- b) The 3-cube Q_3 .



Problem 39.3. For each candidate degree sequence below, either draw a graph with that degree sequence or explain why that list cannot be the degree sequence of a graph.

- a) 4,4,4,4,4
- b) 6,4,4,4,4
- c) 3,2,1,1,1
- d) 3,3,2,2,1

Chapter 40: Trees

Trees are one of the most important classes of graphs. A **tree** is a connected, undirected graph, with no cycles. Consequently, a tree is a simple graph. Moreover, we have

Theorem 40.1. *A graph G is a tree if and only if there is a unique simple path between any two vertices.*

Proof: Suppose that G is a tree and let u and v be two vertices of G . Since G is connected, there is a simple path P of the form $u = v_0, v_1, v_2, \dots, v_n = v$. If Q is a different simple path from u to v , say $u = w_0, w_1, w_2, \dots, w_n = v$ let i be the smallest subscript so that $w_i = v_i$, but so that $v_{i+1} \neq w_{i+1}$. Also, let j be the next smallest subscript where $v_j = w_j$. By construction the path $v_i, v_{i+1}, \dots, v_j, w_{j-1}, w_{j-2}, \dots, w_i$ is a cycle in G . This contradicts G having no cycles.

Conversely, if G is a graph where there is a unique simple path between any pair of vertices, then by definition G is connected. If G contained a cycle, C , then any two vertices of C would be joined by two distinct simple paths. Therefore, G contains no cycles, and is a tree. ■

A consequence of Theorem 40.1 is that given any vertex r in a tree, we can draw T with r at the top and the other vertices in levels below. The neighbors of r thus appear at the first level and are called r 's **children**. The neighbors of r 's children are put in the second level and are r 's **grandchildren**. In general, the i th level consists of those vertices in the tree which are at distance i from r . The result is called a **rooted tree**. A rooted tree is implicitly directed, but we suppress the arrows on edges since every edge is drawn downwards. The **height** of a rooted tree is the maximum level number.

Naturally, besides child and parent, many genealogical terms apply to rooted trees and are suggestive of the structure. For example, if $T = (V, E, r)$ is a rooted tree with root r , and we let $v \in V - \{r\}$, the **ancestors** of v are all vertices on the path from r to v , including r , but excluding v . The **descendants** of a vertex w consist of all vertices which have w as one of their ancestors. The **subtree rooted at w** is the rooted tree consisting of w , its descendants, and all requisite paths. A vertex with no children is a **leaf**, and a vertex with at least one child is called an **internal vertex**.

To distinguish rooted trees by breadth, we use the term **m -ary** to mean that any internal vertex has at most m children. An m -ary tree is **full** if every internal vertex has exactly m children. When $m = 2$, we use the term **binary**.

As an initial application of rooted trees we prove the following theorem.

Theorem 40.2. *A tree on n vertices has $n - 1$ edges.*

Proof: Let $T = (V, E)$ be a tree with n vertices. Let $u \in V$ and form the tree $T = (V, E, u)$ rooted at u . Any edge $e \in E$ joins two vertices v and w where v is the parent of w . This allows us to define a function $f: E \rightarrow V - \{u\}$ by $f(e) = w$. f is one-to-one by uniqueness of simple path from u to w . f is onto by connectivity. Therefore $|E| = |V - \{u\}| = |V| - 1 = n - 1$. ■

We draw as a corollary

Corollary 40.3. *A full m -ary tree with i internal vertices has $n = mi + 1$ vertices.*

Since every vertex in a rooted tree is either internal or a leaf, we know that a full m -ary tree with i internal vertices has $l = (m - 1)i + 1$ leaves. In short, if we know any two of the three quantities n, i and l for a full m -ary tree, we can deduce the third.

A very important application of full, rooted, binary trees is their use to model arithmetic and algebraic expressions. In this case the last operation performed acts as the root. Call this operation $\star$. $\star$ is usually one of addition, subtraction, multiplication, or division. Since order of evaluation matters when we subtract or divide, we need to also order the tree distinguishing each pair of children as left child and right child. Our expression is then modeled as $T_1 \star T_2$, where T_1 is the left child, and each of T_1 and T_2 may be constructed recursively.

Example 40.4. The expression $((x + 2)^3) * (y - (3 + x)) - 5$ is modeled by the tree U .

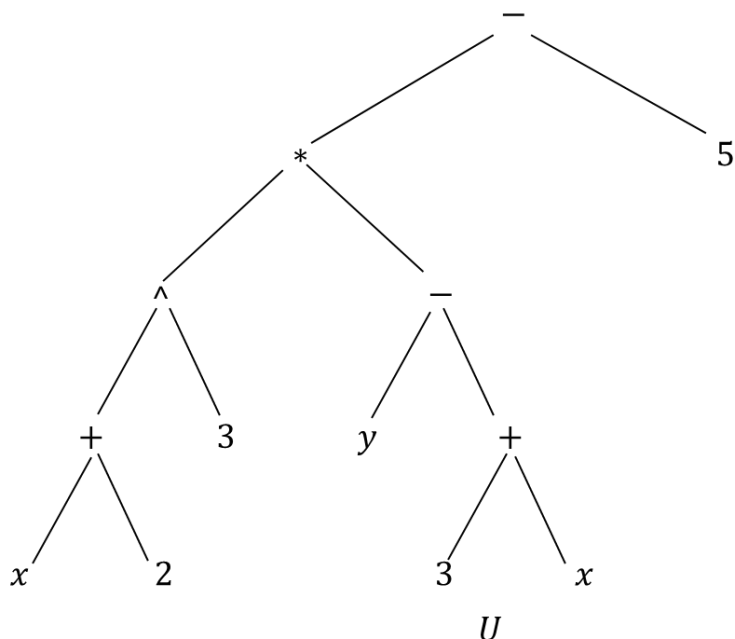


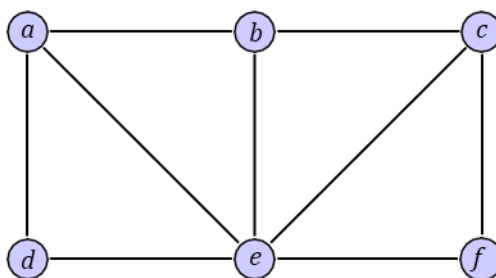
Figure 40.1: A rooted binary tree modeling arithmetic

Of the many algorithms involving graphs and trees. When G is a connected graph one of the most important algorithms builds a connected subgraph T of G which is a tree and contains all of the vertices of G . The subgraph T is called a **spanning tree** of G . More complicated algorithms are concerned with finding a spanning tree with certain properties.

We describe two algorithms for finding a spanning tree for a connected graph G . They use the notions of depth-first search and breadth-first search. The depth-first search algorithm will build a spanning tree with height. Meanwhile, the breadth-first search algorithm will be a spanning tree with less height and vertices of higher degree.

Algorithm 5 Depth-first search for a spanning tree**Input:** *A connected, undirected graph G with vertices ordered $V = (v_1, \dots, v_n)$.***Output:** *The edges in G which form a spanning tree*

- 1: Pick a vertex $p \leftarrow v_1$ (as a pointer) and set $W = (p)$
- 2: Initialize the edge set of the spanning tree $F \leftarrow \emptyset$
- 3: Using the ordering of vertices select the first vertex v_j adjacent to p where adding the edge $\{v_j, p\}$ does not form a cycle.
- 4: Add the edge $\{v_j, p\}$ to F and add the vertex v_j to the ordered tuple W .
- 4: Set $p \leftarrow v_j$ and repeat step 3 until no longer possible.
- 5: If $|F| = n - 1$ we are done.
- 6: Else we backtrack to the previously visited vertex in W and revisit step 3

Example 40.5. *Consider the graph below with order of vertices a, b, c, d, e, f .*

Using the depth-first search algorithm the steps would give rise to

a: $W = (a), F = \emptyset$;

b: $F = \{\{a, b\}\}, W = (a, b), p = b$;

c: $F = \{\{a, b\}, \{b, c\}\}, W = (a, b, c), p = c$;

d: $F = \{\{a, b\}, \{b, c\}, \{c, e\}\}, W = (a, b, c, e), p = e$;

e: $F = \{\{a, b\}, \{b, c\}, \{c, e\}, \{e, d\}\}, W = (a, b, c, e, d), p = d$;

Since no edge out of d can be added without forming a cycle we backtrack setting $p = e$.

f: $F = \{\{a, b\}, \{b, c\}, \{c, e\}, \{e, d\}, \{e, f\}\}, W = (a, b, c, e, d, f), p = f$.

Then we're done since $|F| = 5 = 6 - 1$. The resulting tree has height 4.

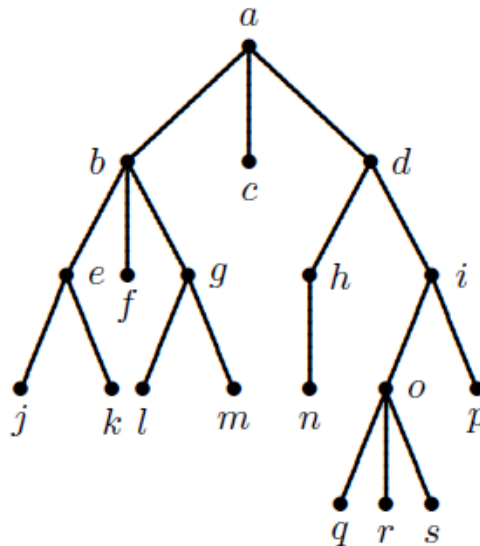
Using the ordering b, a, c, d, e, f we get the tree with edges $\{b, a\}, \{a, d\}, \{d, e\}, \{e, c\}, \{c, f\}$. This tree has height 5.

Example 40.6. Consider the graph from example 40.5 with order of vertices a, b, c, d, e, f . The breadth-first search spanning tree has edges: Round 1: $\{a, b\}, \{a, d\}, \{a, e\}$; Round 2: add $\{b, c\}$; Round 3: add $\{c, f\}$. Meanwhile with ordering e, a, b, c, d, f the tree would be generated in one round with edges $\{e, a\}, \{e, b\}, \{e, c\}, \{e, d\}, \{e, f\}$. The first tree is ternary, while the second tree is pentary.

Problems

Problem 40.1 Answer the following questions about the rooted tree.

- Which vertex is the root
- Which vertex is the parent of m ?
- Which vertices are internal?
- Which vertices are siblings of q ?
- Which vertices are leaves?
- Which vertices are ancestors of p ?
- Which vertices are children of b ?
- Which vertices are descendants of d ?
- Which vertices are grandchildren of b ?
- What level is i at?



Problem 40.2. A tree is called **star-like** if there is exactly one vertex with degree greater than 2. How many different (that is, nonisomorphic) star-like trees are there with six vertices? (Note: If you draw the graph with the vertex of degree greater than 2 having the arms of the tree radiating out from it like spokes on a wheel, the name star-like will make sense.)

Problem 40.3. A forest is a graph consisting of one or more (separate) trees. If the total number of vertices in a forest is f , and the number of trees in the forest is t , what is the total number of edges in the forest?

Appendix A: Solutions to Exercises

Chapter 1 Solutions:

Exercise 1.1. *Determine which statements are propositions.*

Statements a) and d) are propositions; Statements b) and c) are not propositions.

Exercise 1.2. *Construct truth tables.*

a)

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

b)

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

c)

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

d)

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

e)	p	q	r	p	$\rightarrow$	$(\neg$	q	$\wedge$	$r)$
	T	T	T	T	F	F	T	F	T
	T	T	F	T	F	F	T	F	F
	T	F	T	T	T	T	F	T	T
	T	F	F	T	F	T	F	F	F
	F	T	T	F	T	F	T	F	T
	F	T	F	F	T	F	T	F	F
	F	F	T	F	T	T	F	T	T
	F	F	F	F	T	T	F	F	F

Exercise 1.3. Perform bit string operations:

- $(1101\ 0111 \oplus 1110\ 0010) \wedge 1100\ 1000 = (0011\ 0101) \wedge 1100\ 1000 = 0000\ 0000$
- $(1111\ 1010 \wedge 0111\ 0010) \vee (0101\ 0001) = (0111\ 0010) \vee (0101\ 0001) = 0111\ 0011$
- $(1001\ 0010 \vee 0101\ 1101) = (1101\ 1111)$ and
 $(0110\ 0010 \vee 0111\ 0101) = (0111\ 0111)$ so
 $(1001\ 0010 \vee 0101\ 1101) \wedge (0110\ 0010 \vee 0111\ 0101) = 0101\ 0111$

Exercise 1.4. Convert from English to symbols.

- $s \wedge \neg f$
- $f \wedge \neg s$
- $\neg s \rightarrow \neg f$

Exercise 1.5. Convert from symbols to English.

- Jordan did not play and the Wizards won.
- If Jordan played, then the Wizards lost.
- The Wizards won or Jordan played.
- Jordan didn't play when the Wizards won. aka If the Wizards won, then Jordan didn't play.

Exercise 1.6. Translate between English and symbols.

- If Sam plays chess with the white pieces, she wins.
- $(c \wedge \neg w) \rightarrow b$

Chapter 2 Solutions:

Exercise 2.1. Use truth tables to show logical equivalence.

a)

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

b)

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

c)

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

Exercise 2.2. Use truth tables to show propositions are not logically equivalent.

a)

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

Consider $(p, q, r) = (F, T, T)$ where $p \wedge (q \rightarrow r) = F$ while $(p \wedge q) \rightarrow r = T$.

b)

p	q	$p \rightarrow q$	$q \rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	F

Consider $(p, q) = (T, F)$ where $p \rightarrow q = F$ while $q \rightarrow p = T$.

c)

p	q	$p \rightarrow q$	$\neg p \rightarrow \neg q$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Consider $(p, q) = (T, F)$ where $p \rightarrow q = F$ while $\neg p \rightarrow \neg q = T$.

Exercise 2.3. Use a truth table to show a proposition is a tautology.

a)

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

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

Exercise 2.4. Write converse, inverse and contrapositive in English.

- If I mow the lawn, then it is Saturday.
- If it is not Saturday, then I do not mow the lawn.
- If I do not mow the lawn, then it is not Saturday.

Exercise 2.5. Determine equivalences among implication, converse, inverse and contrapositive.

An implication is logically equivalent to its contrapositive. (If it is Saturday, then I mow the lawn.) is logically equivalent to (If I do not mow the lawn, then it is not Saturday.). The inverse and converse of an implication are logically equivalent (but not logically equivalent to the implication).

Exercise 2.6. Find assignments of truth values to show a compound proposition is not a tautology.

- When $(p, q, r) = (T, F, F)$ then $(p \wedge q) \rightarrow r = T \neq F = [(p \rightarrow r) \wedge (q \rightarrow r)]$.
- When $(p, q, r) = (F, T, T)$ then $[(p \wedge q) \vee r] = T \neq F = [p \wedge (q \vee r)]$.

Exercise 2.7. Give a proof that $(p \wedge \neg r) \rightarrow \neg q \equiv p \rightarrow (q \rightarrow r)$ using Logical Equivalences.

$$\begin{aligned}
 \text{Proof. } (p \wedge \neg r) \rightarrow \neg q &\equiv \neg(p \wedge \neg r) \vee \neg q && \text{Disjunctive or-form} \\
 &\equiv (\neg p \vee \neg \neg r) \vee \neg q && \text{DeMorgan's Law} \\
 &\equiv (\neg p \vee r) \vee \neg q && \text{Double Negation Law} \\
 &\equiv \neg p \vee (r \vee \neg q) && \text{Associative Law} \\
 &\equiv \neg p \vee (\neg q \vee r) && \text{Commutative Law} \\
 &\equiv \neg p \vee (q \rightarrow r) && \text{Disjunctive or-form} \\
 &\equiv p \rightarrow (q \rightarrow r) \blacksquare && \text{Disjunctive or-form}
 \end{aligned}$$

Chapter 3 Solutions:

Exercise 3.1. Determine the truth value of a bound propositional function – proposition.

Parts a) and d) are T b) is clearly F while c) is false since $(0 \leq 10) \rightarrow (2 \cdot 0 \geq 4)$ is false.

Exercise 3.2. Convert statements from symbols to English.

- a) Everyone in class has read *War and Peace*.
- b) Someone in class has not read *The Great Gatsby*.
- c) Someone in class has read every novel.
- d) For each novel there is at least one person in the class who has not read that novel.

Exercise 3.3. Convert statements from English to symbols.

- a) $\forall y F(I, y)$
- b) $\neg \exists y F(\text{George}, y) \equiv \forall y \neg F(\text{George}, y)$
- c) $\nexists x F(x, x) \equiv \forall x \neg F(x, x)$
- d) $\exists x \forall y F(x, y)$
- e) $\exists y \forall x F(x, y)$
- f) $\exists y \exists z ((y \neq z) \wedge F(\text{Ralph}, y) \wedge F(\text{Ralph}, z))$

Exercise 3.4. Negate statements in English.

- a) Someone in class has not read *War and Peace*.
- b) Everyone in class has the *The Great Gatsby*.
- c) No student in class has read every novel.
- d) There is a novel that no one in class has read.

Exercise 3.5. Negate statements in symbolic form.

- a) $\exists y \neg F(I, y)$
- b) $\exists y F(\text{George}, y)$
- c) $\exists x F(x, x)$
- d) $\forall x \exists y \neg F(x, y)$
- e) $\forall y \exists x \neg F(x, y)$
- f) 1st solution: $\forall y \forall z (y = z) \vee \neg F(\text{Ralph}, y) \vee \neg F(\text{Ralph}, z)$.

In English: Pick two people (not necessarily distinct). Either they are the same person, or else Ralph cannot fool at least one of the two.

2nd solution: $\forall y \forall z ((F(\text{Ralph}, y) \wedge F(\text{Ralph}, z)) \rightarrow (y = z))$.

In English: Ralph can fool at most one person.

Or less preferable: If Ralph can fool both y and z , then y and z are the same person.

Exercise 3.6. Express a statement symbolically.

$\forall x \forall y ((E(x) \wedge O(y)) \rightarrow E(x \cdot y))$, where $E(x)$: x is an even integer and $O(y)$: y is an odd integer.

Exercise 3.7. Express a symbolic statement in English.

1st solution: There is an x so that $P(x)$ holds and for any x and y if both $P(x)$ and $P(y)$ hold, then x and y are equal.

2nd solution (preferable): There is exactly one x for which $P(x)$ is true.

Chapter 4 Solutions:

Exercise 4.1. Validate a rule of inference.

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

The statement is a tautology, hence a valid rule of inference.

Exercise 4.2. Prove an argument in English statements is valid.

Proof. Make the assignments Porsche(x): “ x owns a Porsche”, Speeder(x): “ x is a speeder”, Sedan(x): “ x owns a sedan”, and BuysPrem(x): “ x buys premium fuel”. The argument has the symbolic form:

$$\begin{array}{l}
 \forall x (\text{Porsche}(x) \rightarrow \text{Speeder}(x)) \\
 \neg \exists x (\text{Sedan}(x) \wedge \text{BuysPrem}(x)) \\
 \forall x (\neg \text{BuysPrem}(x) \rightarrow \neg \text{Speeder}(x)) \\
 \hline
 \therefore \forall x (\text{Porsche}(x) \rightarrow \neg \text{Sedan}(x))
 \end{array}$$

The steps of the proof in two-column form with justifications is below.

1: $\forall x(\text{Porsche}(x) \rightarrow \text{Speeder}(x))$	Premise
2: $\text{Porsche}(c) \rightarrow \text{Speeder}(c)$	Universal Instantiation, 1
3: $\forall x (\neg \text{BuysPrem}(x) \rightarrow \neg \text{Speeder}(x))$	Premise
4: $\neg \text{BuysPrem}(c) \rightarrow \neg \text{Speeder}(c)$	Universal Instantiation, 3
5: $\text{Speeder}(c) \rightarrow \text{BuysPrem}(c)$	Contrapositive, 4
6: $\text{Porsche}(c) \rightarrow \text{BuysPrem}(c)$	Hypothetical Syllogism, 2 and 5
7: $\neg \exists x (\text{Sedan}(x) \wedge \text{BuysPrem}(x))$	Premise
8: $\forall x \neg (\text{Sedan}(x) \wedge \text{BuysPrem}(x))$	DeMorgan's Law, 7
9: $\neg (\text{Sedan}(c) \wedge \text{BuysPrem}(c))$	Universal Instantiation
10: $\neg \text{Sedan}(c) \vee \neg \text{BuysPrem}(c)$	DeMorgan's Law, 9
11: $\neg \text{BuysPrem}(c) \vee \neg \text{Sedan}(c)$	Commutative Law, 10
12: $\text{BuysPrem}(c) \rightarrow \neg \text{Sedan}(c)$	Disjunctive or-form, 11
13: $\text{Porsche}(c) \rightarrow \neg \text{Sedan}(c)$	Hypothetical Syllogism, 6 and 12
14: $\therefore \forall x (\text{Porsche}(x) \rightarrow \neg \text{Sedan}(x))$	Universal Generalization, 13

Exercise 4.3. *Prove a symbolic argument is valid.*

In two-column form with justifications an argument for validity is:

1: $\neg w$	Premise
2: $u \vee w$	Premise
3: u	Disjunctive Syllogism, 1 and 2
4: $u \rightarrow \neg p$	Premise
5: $\neg p$	Modus Ponens, 3 and 4
6: $\neg p \rightarrow (r \wedge \neg s)$	Premise
7: $r \wedge \neg s$	Modus Ponens, 5 and 6
8: $\neg s$	Simplification, 7
9: $t \rightarrow s$	Premise
10: $\neg t$	Modus Tollens, 8 and 9
11: $\neg t \vee w$	Addition, 10

Chapter 5 Solutions:

Exercise 5.1. *List the elements of certain sets.*

- a) $\{2,3,4\}$
- b) $\{-5,5\}$
- c) $\{4,5,6\}$

Exercise 5.2. *Use set-builder notation to describe sets.*

- a) $\{5x | x \in \mathbb{Z} \text{ where } -1 \leq x \leq 3\}$
- b) $\{x | x \in \mathbb{N} \text{ where } x \leq 4\}$ or $\{x | x \in \mathbb{Z} \text{ where } -1 < x < 5\}$
- c) $\{x \in \mathbb{R} | \pi \leq x \leq 4\}$ or $\{x | x \in \mathbb{R} \text{ where } \pi \leq x \leq 4\}$

Exercise 5.3. *Determine the cardinality of sets.*

- a) $|\{x \in \mathbb{Z} | 3 \leq x^3 < 100\}| = 3 = |\{2,3,4\}|$
- b) $|\{-5,5\}| = 2$
- c) $|\{4,5,6\}| = 3$
- d) $|\{-5,0,5,10,15\}| = 5$
- e) $|\{0,1,2,3,4\}| = 5$
- f) The interval $[\pi, 4)$ has infinite cardinality.

Exercise 5.4. *Answer T/F with explanation “Every element of the empty set has three toes.”*

Rewrite the statement as “If $x \in \emptyset$, then x has three toes.”

Because the hypothesis is false, this implication is true.

Exercise 5.5. *Determine the power set of $\{1, \{2\}\}$.*

$$\mathcal{P}(\{1, \{2\}\}) = \{\emptyset, 1, \{2\}, \{1, \{2\}\}\}$$

Exercise 5.6. *T or F: $\{1,2,3,4,5\} = \{5,2,3,1,2,1,5,4,3,2,1\}$.*

This is true since repetition and order don't matter when listing elements of a set.

Exercise 5.7. *T/F: The set of even integers is a subset of the set of integers that are multiples of four.*

This is false. For example, 2 is in the set of even integers, but not in the set of integers that are multiples of 4. In fact, the reverse statement is true: Every integer that is a multiple of 4 is a multiple of 2. So, the set of integers that are multiples of 4 is a subset of the set of integers that are even.

Chapter 6 Solutions:

Exercise 6.1. Perform set operations.

- a) $A \cap B = \{2, 4, 6, 7, 8\}$
- b) $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- c) $A - B = \{3, 5\}$
- d) $B - A = \{1, 9\}$

Exercise 6.2. Determine A and B given $A - B$, $B - A$ and $A \cap B$.

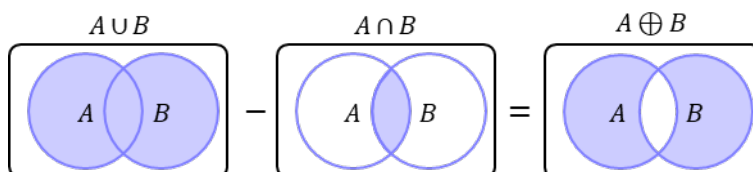
- a) $A = (A - B) \cup (A \cap B) = \{1, 2, 5, 6, 7, 8, 9\}$
- b) $B = (B - A) \cup (A \cap B) = \{3, 4, 5, 6, 9, 10\}$

Exercise 6.3. Use set membership tables to prove a law of set theory.

A	B	A	$\oplus$	B	$(A \cup B)$	$-$	$(A \cap B)$
1	1	1	0	1	1	1	1
1	0	1	1	0	1	0	0
0	1	0	1	1	0	1	0
0	0	0	0	0	0	0	0

The columns in red are identical and that shows the set equality is correct.

Exercise 6.4. Verify $A \oplus B = (A \cup B) - (A \cap B)$ using Venn diagrams.



Exercise 6.5. Verify $A \cup (A \cap B) = A$ using the rules of set algebra.

Let $\mathcal{U}$ denote the universal set.

$$\begin{aligned}
 \text{Proof. } A \cup (A \cap B) &= (A \cap \mathcal{U}) \cup (A \cap B) && \cap - \text{Identity law} \\
 &= A \cap (\mathcal{U} \cup B) && \text{Distributive Law} \\
 &= A \cap \mathcal{U} && \cup - \text{Domination Law} \\
 &= A && \cap - \text{Identity law}
 \end{aligned}$$

Exercise 6.6. Write out Cartesian products.

- a) $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c), (4, a), (4, b), (4, c)\}$
- b) $B \times A = \{(a, 1), (a, 2), (a, 3), (a, 4), (b, 1), (b, 2), (b, 3), (b, 4), (c, 1), (c, 2), (c, 3), (c, 4)\}$
- c) $C \times B \times D = \{(\alpha, a, 7), (\alpha, a, 8), (\alpha, a, 9), (\alpha, b, 7), (\alpha, b, 8), (\alpha, b, 9), (\alpha, c, 7), (\alpha, c, 8), (\alpha, c, 9), (\beta, a, 7), (\beta, a, 8), (\beta, a, 9), (\beta, b, 7), (\beta, b, 8), (\beta, b, 9), (\beta, c, 7), (\beta, c, 8), (\beta, c, 9)\}$

Exercise 6.7. *What can you conclude about A and B if $A \times B = B \times A$?*

We can conclude that $A = \emptyset, B = \emptyset$ or $A = B$.

Exercise 6.8. *Determine the characteristic vector of a set.*

$\chi(\{1,2,4,8\}) = 0110100010$ with respect to the given ordering.

Exercise 6.9. *List the elements of a subset of a Cartesian product.*

The elements in the subset B are $(1,1), (2,1), (2,2), (3,1), (3,2), (3,3)$.

Chapter 7 Solutions:

Exercise 7.1. *Give a direct proof that the sum of two even integers is even.*

We present the list form of the proof, followed by the prose form of the proof.

Proof. 1: Let $m, n \in \mathbb{Z}$ be given.

2: Suppose that m and n are even.

Hypothesis

3: $\Rightarrow m = 2i$ and $n = 2j \exists i, j \in \mathbb{Z}$

Definition of even

4: $\Rightarrow m + n = 2i + 2j = 2(i + j)$

Algebra

5: $\Rightarrow m + n = 2l$, where $l = i + j \in \mathbb{Z}$

Algebra

6: $\Rightarrow m + n$ is even

Definition of Even

7: $\therefore$ If m and n are even, then $m + n$ is even. ■

Proof. Suppose that m and n are even integers. Then by definition of even $m = 2i$ and $n = 2j$ for some integers i, j . Thus we have

$$m + n = 2i + 2j = 2(i + j) = 2l, \text{ where } l = i + j \in \mathbb{Z}.$$

Hence $m + n$ is even by definition. ■

Exercise 7.2. *Give an indirect proof that if the square of an integer n is odd, then n is odd.*

Symbolically we have

$$\begin{aligned} (\forall n \in \mathbb{Z})[(n^2 \text{ is odd}) \rightarrow (n \text{ is odd})] &\equiv (\forall n \in \mathbb{Z})[\neg(n \text{ is odd}) \rightarrow \neg(n^2 \text{ is odd})] \\ &\equiv (\forall n \in \mathbb{Z})[(n \text{ is even}) \rightarrow (n^2 \text{ is even})] \end{aligned}$$

We present the prose form of the proof, followed by the list form of the proof.

Proof. Suppose that n is an even integer. Then by definition of even $n = 2j$ for some $j \in \mathbb{Z}$. Thus, $n^2 = (2j)^2 = 2^2 j^2 = 2(2j^2) = 2l$, where $l = 2j^2 \in \mathbb{Z}$. Hence n^2 is even. ■

Proof. 1: Let $n \in \mathbb{Z}$ be given.

2: Suppose that n is even. Hypothesis

3: $\Rightarrow n = 2j \exists j \in \mathbb{Z}$ Definition of even

4: $\Rightarrow n^2 = (2j)^2$ Algebra

5: $\Rightarrow n^2 = 2(2j^2) = 2l$, where $l = 2j^2 \in \mathbb{Z}$ Algebra

6: $\Rightarrow n^2$ is even Definition of Even

7: $\therefore$ If n is even, then n^2 is even. ■

Exercise 7.3. Give a proof by contradiction that the sum of a rational number and an irrational number is irrational.

$(\forall x, y \in \mathbb{R})[(x \text{ is rational}) \wedge (y \text{ is irrational}) \rightarrow (x + y \text{ is irrational})]$

$\equiv (\forall x, y \in \mathbb{R})[(x \text{ is rational}) \wedge (y \text{ is irrational}) \wedge \neg(x + y \text{ is irrational}) \rightarrow \mathbb{F}]$

$\equiv (\forall x, y \in \mathbb{R})[(x \text{ is rational}) \wedge (y \text{ is irrational}) \wedge (x + y \text{ is rational}) \rightarrow \mathbb{F}]$

We present the list form of the proof first, followed by the prose form of the proof.

Proof. 1: Let $x, y \in \mathbb{R}$ be given.

2: Suppose that x is rational and y is irrational. Premise

3: Suppose that $x + y$ is also rational Premise

4: $\Rightarrow y = (x + y) - x$ is rational Difference of rational numbers is rational

5: $\Rightarrow y$ is rational $\wedge y$ is irrational $\rightarrow \leftarrow$ Conjunction 2, 4

7: $\therefore$ If $x + y$ must be irrational. ■

Proof. Suppose that x is rational and y is irrational. Suppose for the sake of argument that $x + y$ is rational. Then $y = (x + y) - x$ is rational (see below), since the difference of two rational number is rational. But y was given to be irrational. This is impossible. Therefore $x + y$ must have been irrational. ■

One might add the argument that if $r, s, t, u \in \mathbb{Z}$ with $s, u \neq 0$, then $\frac{r}{s} - \frac{t}{u} = \frac{ru - st}{su} = \frac{p}{q}$ where we have $p = ru - st, q = su \in \mathbb{Z}$ and $su \neq 0$.

Exercise 7.4. Give a proof by contradiction that if $5n - 1$ is odd, then n is even.

$$\begin{aligned} (\forall n \in \mathbb{Z})[(5n - 1 \text{ is odd}) \rightarrow (n \text{ is even})] &\equiv (\forall n \in \mathbb{Z})[(5n - 1 \text{ is odd}) \wedge \neg(n \text{ is even})] \rightarrow \mathbb{F}] \\ &\equiv (\forall n \in \mathbb{Z})[(5n - 1 \text{ is odd}) \wedge (n \text{ is odd})] \rightarrow \mathbb{F}] \end{aligned}$$

We present the list form of the proof first, followed by the prose form of the proof.

<i>Proof.</i>	1: Let $n \in \mathbb{Z}$ be given.	
	2: Suppose that $5n - 1$ is odd	Premise
	3: Suppose that n is also odd	Premise
	4: $\Rightarrow n = 2j + 1$ for some $j \in \mathbb{Z}$	Definition of odd
	5: $\Rightarrow 5n - 1 = 5(2j + 1) - 1$	Substitution
	6: $\Rightarrow 5n - 1 = 10j + 5 - 1$	Algebra
	7: $\Rightarrow 5n - 1 = 10j + 4$	Arithmetic
	8: $\Rightarrow 5n - 1 = 2(5j + 2)$	Algebra
	9: $\Rightarrow 5n - 1 = 2l$ where $l = 5j + 2 \in \mathbb{Z}$	Substitution
	10: $\Rightarrow 5n - 1$ is even.	Definition of even
	11: $(5n - 1 \text{ is even}) \wedge (5n - 1 \text{ is odd}) \rightarrow \mathbb{F}$	Conjunction 2,10
	12: $\therefore$ If n must be even. ■	

Proof. Suppose that $5n - 1$ is odd for some integer n . For the sake of argument suppose that the integer n is odd. Thus, $n = 2j + 1$ for some integer j . So

$$5n - 1 = 5(2j + 1) - 1 = 10j + 5 - 1 = 10j + 4 = 2(5j + 2) = 2l$$

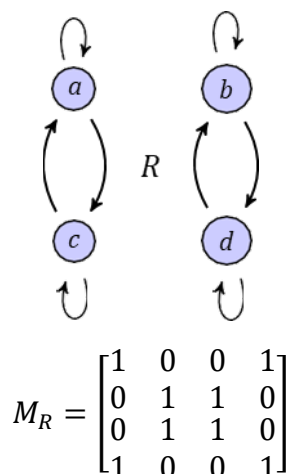
where $l = 5j + 2 \in \mathbb{Z}$. Thus $5n - 1$ is even. But this is impossible since $5n - 1$ was given to be odd. Therefore, we must have that n is even. ■

Exercise 7.5. Give a specific counterexample to the proposition: Every integer that ends in 7 is a prime.

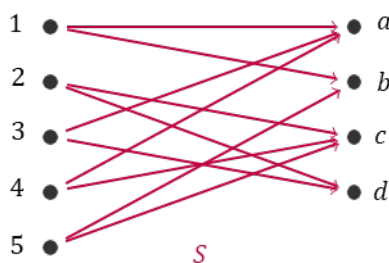
The positive integer 77 ends in a 7, but it is not prime since $77 = 7 \cdot 11$.

Chapter 8 Solutions:

Exercise 8.1. Draw a digraph for a relation. Find the matrix with respect to the ordering d, c, a, b ,



Exercise 8.2. Given the matrix of a relation, represent the relation as a bipartite graph.



Exercise 8.3. Find the composition of two relations as a set of ordered pairs. Then use the Boolean product to find a matrix for the composition.

$$R \circ S = \{(1, a), (1, b), (1, c), (1, d), (2, a), (2, b), (2, c), (2, d), (3, a), (3, b), (3, c), (3, d), (4, a), (4, b), (5, a), (5, b), (5, c), (5, d)\}$$

$$M_{R \circ S} = M_S \odot M_R = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Exercise 8.4. Perform set operations on relations and manipulate their 0,1 –matrices.

$$R_1 \cup R_2 = \{(1, 2), (1, 3), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (3, 1), (3, 3), (3, 4), (3, 6), (4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (5, 1), (5, 5), (5, 6), (6, 2), (6, 3), (6, 6)\}$$

$$R_1 \cap R_2 = \{(1, 2), (2, 1), (2, 2), (3, 3), (5, 5), (6, 6)\}$$

$$R_1 \oplus R_2 = \{(1, 3), (1, 5), (1, 6), (2, 3), (2, 4), (2, 5), (3, 1), (3, 4), (3, 6), (4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (5, 1), (5, 6), (6, 2), (6, 3)\}$$

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$M_{R_1 \oplus R_2} = M_{R_1} \oplus M_{R_2} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Chapter 9 Solutions:

Exercise 9.1. Give an example of a relation on $\{1, 2, 3\}$ which is symmetric and antisymmetric.

$R = \{(1, 1), (2, 2), (3, 3)\}$ or any subset of R .

Exercise 9.2. Determine the properties of a relation on a finite set.

- R is not reflexive since, for example $(1, 1) \notin R$.
- R is irreflexive since none of $(1, 1), (2, 2), (3, 3), (4, 4)$ are in R .
- R is symmetric since the reverse of each ordered pair in R is also in R .
- R is not antisymmetric since, for example, $(1, 2)$ and $(2, 1)$ are both in R , but $1 \neq 2$.
- R is not transitive since, for example, $(1, 2)$ and $(2, 3)$ are both in R , but $(1, 3)$ is not in R .

Exercise 9.3. Given a matrix for a relation, determine which properties the relation has.

- reflexive, not irreflexive, symmetric, not antisymmetric, transitive
- not reflexive, not irreflexive, not symmetric, antisymmetric, transitive
- not reflexive, not irreflexive, symmetric, not antisymmetric, not transitive
- reflexive, not irreflexive, symmetric, not antisymmetric, transitive

Exercise 9.4. Determine the properties of the relation “ A has cardinality less than or equal to the cardinality of B ”.

- a) C is reflexive since any set A has the same number of elements as itself!
- b) C is not irreflexive since, for example, $|\{1\}| = |\{1\}|$ so, $\{1\} C \{1\}$ is true.
- c) C is not symmetric since, for example, $\{1\} C \{1, 2\}$ is true, but $\{1, 2\} C \{1\}$ is false.
- d) C is not antisymmetric since, for example, $\{1\} C \{2\}$ and $\{2\} C \{1\}$ are both true, but $\{1\} \neq \{2\}$.
- e) C is transitive since if $|A| \leq |B|$ and $|B| \leq |D|$, then $|A| \leq |D|$ (by the transitive property of the *less than or equal to* relation for numbers).

Exercise 9.5. Explain why $\emptyset$ is a relation on any set.

For any universe of discourse $\mathcal{U}$, a relation on $\mathcal{U}$ is defined to be any subset of $\mathcal{U} \times \mathcal{U}$. The empty set is a subset of $\mathcal{U} \times \mathcal{U}$.

Exercise 9.6. Determine the properties of a relation on an infinite set.

$\{1, 2\} M \{1, 2\}$ is false, so M is not reflexive.

$\{1\} M \{1\}$ is true, so M is not irreflexive.

If $|A \cap B| = 1$, then $|B \cap A| = 1$, (since $A \cap B = B \cap A$), so M is symmetric.

$\{1\} M \{1, 2\}$ and $\{1, 2\} M \{1\}$ are true, but $\{1\} \neq \{1, 2\}$ so M is not antisymmetric.

$\{1\} M \{1, 2\}$ and $\{1, 2\} M \{2\}$ are true, but $\{1\} M \{2\}$ is false, so M is not transitive.

Chapter 10 Solutions:

Exercise 10.1. Determine if a given relation is an equivalence relation. Determine the equivalence classes if it is an equivalence relation.

The relation R is reflexive since $(0,0), (1,1), (2,2)$ are all in R . R is symmetric since the reverse of each ordered pair in R is also in R . Finally, R is transitive (there are a lot of cases to check for this condition. For example, $(1, 1)$ and $(1, 0)$ are both in R , so we need to check that $(1, 0)$ is also in R . But it is of course. There is a total of nine such checks needed to verify that R is transitive, but they are all just as automatic as that one.) Alternatively, the transitive property follows from verifying $M_R \odot M_R \leq M_R$. So, R is an equivalence relation on A . There are two equivalence classes: $[0] = [1] = \{0, 1\}$ and $[2] = \{2\}$.

Exercise 10.2. Determine if a given relation is an equivalence relation. Determine the equivalence classes if it is an equivalence relation.

The relation R is not reflexive on A since $(3,3) \notin R$. Hence, R is not an equivalence relation on A . It is true that R is symmetric and transitive.

Exercise 10.3. *Determine if a given relation is an equivalence relation. Determine the equivalence classes if it is an equivalence relation.*

The relation R is not symmetric on A since $(1,0) \in R$, but $(0,1) \notin R$. Hence, R is not an equivalence relation on A . It is true that R is reflexive and transitive.

Exercise 10.4. *Determine if a given relation is an equivalence relation. Determine the equivalence classes if it is an equivalence relation.*

The relation R is not transitive on A since $(0,1)$ and $(1,2)$ are in R , but $(0,2) \notin R$. So, R is not an equivalence relation on A . Notice that R is reflexive on A and is symmetric.

Exercise 10.5. *T/F: The relation $R = \{(1,1), (2,2)\}$ on $\{1,2\}$ is both symmetric and antisymmetric?*

True. The relation is symmetric since the reverse of each ordered pair in R is also in R (after all, the reverse of each ordered pair in R is just the ordered pair itself). To check the antisymmetric condition, we need to look at all cases where an ordered pair and its reverse are both in R and make sure the two coordinates are equal in each such case. There are only two cases to check: $(1,1)$ and its reverse are both in R , and sure enough, $1 = 1$. The story is the same for $(2,2)$. So, R passes the antisymmetry test. The moral of the story: It is possible for a relation to be both symmetric and antisymmetric.

Exercise 10.6. *Is a given relation on the integers an equivalence relation? If so, describe the equivalence classes.*

The relation S is reflexive since for any integer m , $m^2 = m^2$. The relation S is symmetric since if $m^2 = n^2$, then $n^2 = m^2$. Finally, S is transitive since if $m^2 = n^2$ and $n^2 = t^2$, then $m^2 = t^2$. So S is an equivalence relation on $\mathbb{Z}$.

The equivalence class of an integer m is the set of all integers with the same square as m . For the case $m = 0$, the only element in the equivalence class would be 0 itself: $[0] = \{0\}$. For any nonzero integer m we get $[m] = \{m, -m\}$. For example, $[2] = \{2, -2\}$ since $2^2 = 4 = (-2)^2$.

Exercise 10.7. *Is a given relation on the lines in the Cartesian plane an equivalence relation? If so, describe the equivalence classes.*

The relation C is obviously reflexive and symmetric. But it is not transitive: The lines $l_1: y = x$ and $l_2: x + y = 2$ intersect at the point $(1,1)$. The lines $l_2: x + y = 2$ and $l_3: y = x + 2$ intersect at the point $(0,2)$. But the lines $l_1: y = x$ and $l_3: y = x + 2$ do not intersect since they are distinct parallel lines. In relation-speak $l_1 C l_2$ and $l_2 C l_3$ are true, but $l_1 C l_3$ is false.

Exercise 10.8. *Prove that if a relation R on a nonempty set A is symmetric, transitive and for each $a \in A$ there is (at least one) $b \in A$ with aRb , then the relation R is reflexive.*

Premises: R is symmetric: $\forall a, b \in A, aRb \rightarrow bRa$;

R is transitive: $\forall a, b, c \in A$,

$(aRb \wedge bRc) \rightarrow aRc$; $\forall a \in A \exists b \in A aRb$.

Conclusion: $\forall a \in A, aRa$.

<i>Proof.</i> 1: Let $a \in A$ be given	Universal Instantiation
2: $\exists b \in A$ with aRb	Premise
3: bRa	Premise (R is symmetric)
4: $aRb \wedge bRa$	Conjunction 2,3
5: aRa	Transitivity and 4
6: R is reflexive	Universal Generalization
7: R is an equivalence relation ■	Premises and 6

Exercise 10.9. Given an equivalence relation E on a set A prove that $[a] \cap [b] = \emptyset$ or else $[a] = [b]$.

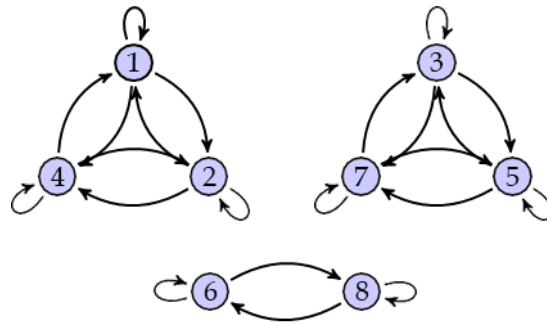
We need the definition $[a] \subseteq [b] \equiv (\forall x \in [a] \rightarrow x \in [b])$ and the equivalencies

$$\begin{aligned} \forall a, b \in A, [([a] \cap [b] = \emptyset) \vee ([a] = [b])] &\equiv \forall a, b \in A, [\neg ([a] \cap [b] = \emptyset) \rightarrow ([a] = [b])] \\ &\equiv \forall a, b \in A, [([a] \cap [b] \neq \emptyset) \rightarrow ([a] = [b])] \\ &\equiv \forall a, b \in A, [([a] \cap [b] \neq \emptyset) \rightarrow ([a] \subseteq [b] \wedge [b] \subseteq [a])] \end{aligned}$$

<i>Proof.</i> 1: Let $a, b \in A$ be given.	Universal Instantiation
2: Suppose $[a] \cap [b] \neq \emptyset$	Hypothesis
3: $\exists c \in [a] \cap [b]$	Definition of nonempty
4: $c \in [a] \wedge c \in [b]$	Definition of Intersection
5: $cEa \wedge cEb$	Definition of Equivalence Class
6: $aEc \wedge bEc$	Symmetry of E
7: aEc	Simplification, 6
8: bEc	Simplification, 6
$[a] \subseteq [b]$: 9: Let $x \in [a]$	Universal Instantiation
10: xEa	Definition of Equivalence Class
11: $xEa \wedge aEc$	Conjunction, 10 and 7
12: xEc	Transitivity of E , 11
13: cEb	Simplification, 5
14: $xEc \wedge cEb$	Conjunction, 12 and 13

15. xEb	Transitivity of E , 14
16. $x \in [b]$	Definition of $[b]$
17. $\therefore x \in [a] \rightarrow x \in [b]$	Modus Ponens, 9 and 16
$[b] \subseteq [a]$: 18. Let $x \in [b]$	Universal Instantiation
19: xEb	Definition of Equivalence Class
20. $xEb \wedge bEc$	Conjunction, 19 and 8
21. xEc	Transitivity of E , 20
22. cEa	Simplification, 5
23. $xEc \wedge cEa$	Conjunction, 21 and 22
24. xEa	Transitivity of E , 23
25. $x \in [a]$	Definition of $[a]$
26. $\therefore x \in [b] \rightarrow x \in [a]$	Modus Ponens, 18 and 25

Exercise 10.10. Given the parts of a partition (equivalence classes), represent the corresponding equivalence relation as a digraph and via a 0,1 –matrix.



Using the natural order $[1, 2, 3, 4, 5, 6, 7, 8]$:

$$M_E = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Using an order grouped by equivalence classes $[1, 2, 4], [3, 5, 7], [6, 8]$:

$$M_E = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Exercise 10.11. Determine if a matrix represents an equivalence relation.

- $[a] = \{a, c, e, g\} = [c] = [e] = [g]$, $[b] = \{b, d, f\} = [d] = [f]$ and $[h] = \{h\}$ partition A .
- $[a] = \{a, b, g, h\} = [b] = [g] = [h]$, $[c] = \{c, d\} = [d]$ and $[e] = \{e, f\} = [f]$ partition A .

Exercise 10.12. Complete the proof of theorem 10.7 on page 67 by proving part 1.

We have that E is an equivalence relation on the set A and that $a \in [b]$. (a is in the equivalence class of b). Our job is to show that if $c \in [a]$, then $c \in [b]$. So let $c \in [a]$. That means cEa is true according to the definition of equivalence class. We also know aEb is true, since a is in the equivalence class of b . Since cEa and aEb are true, the transitive condition tells us cEb is true, and that means $c \in [b]$. ■

Chapter 11 Solutions:

Exercise 11.1. If possible, give examples of functions with domain and codomain $\mathbb{R}$.

There are many answers to each part.

- $f(x) = x + 1$ is bijective, but not $1_{\mathbb{R}}$.
- $f(x) = 1$ is neither one-to-one nor onto.
- $f(x) = e^x$ is one-to-one, but not onto $\mathbb{R}$.
- $f(x) = x^3 - x$ is onto $\mathbb{R}$, but not one-to-one, since $f(0) = f(1) = 0$.

Exercise 11.2. If possible, give examples of functions with finite domain and finite codomain.

- As a set of ordered pairs $f = \{(1, a), (2, b), (3, c), (4, d), (5, e)\}$ is one-to-one from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c, d, e, f\}$.
- No one-to-one function exists since $6 = |B| > |A| = 5$.
- No onto function exists since $5 = |A| < |B| = 6$.
- As a set of ordered pairs $g = \{(a, 1), (b, 2), (c, 3), (d, 4), (e, 5), (f, 5)\}$ is an onto function from $\{a, b, c, d, e, f\}$ to $\{1, 2, 3, 4, 5\}$.

Exercise 11.3. *Prove or give a counterexample: If E is an equivalence relation on A , then $E \circ E$ is also an equivalence relation on A .*

In general, the composition of two equivalence relations need not be an equivalence relation. However, we can prove: If E is an equivalence relation on A , then $E \circ E$ is also an equivalence relation on A .

Proof. Suppose E is an equivalence relation on a set A .

Since E is reflexive on A , for any $a \in A$, $(a, a) \in E$ is true, and since (a, a) and (a, a) are in E , the composition rule tells us $(a, a) \in E \circ E$. So $E \circ E$ is reflexive on A . Next, suppose $(a, b) \in E \circ E$. That means there is an x in A such that (a, x) and (x, b) are in E . Since E is an equivalence relation, it is symmetric, so (b, x) and (x, a) are in E . The composition rule then tells us (b, a) is in $E \circ E$. That proves $E \circ E$ is symmetric. Finally, suppose (a, b) and (b, c) are in $E \circ E$. That means there is an x in A such that (a, x) and (x, b) are in E and there is a y in A such that (b, y) and (y, c) are in E . From (x, b) and (b, y) in E , we see (x, y) is in E . Then from (a, x) and (x, y) in E , we get (a, y) is in E . And finally, (a, y) and (y, c) in E tells us (a, c) is in $E \circ E$. So $E \circ E$ is transitive.

Exercise 11.4. *Prove that the composition of one-to-one functions is one-to-one.*

Suppose that $g: A \rightarrow B$ and $f: B \rightarrow C$ are both one-to-one. To show $f \circ g: A \rightarrow C$ is one-to-one, suppose x and y are in A and $(f \circ g)(x) = (f \circ g)(y)$. We want to show $x = y$.

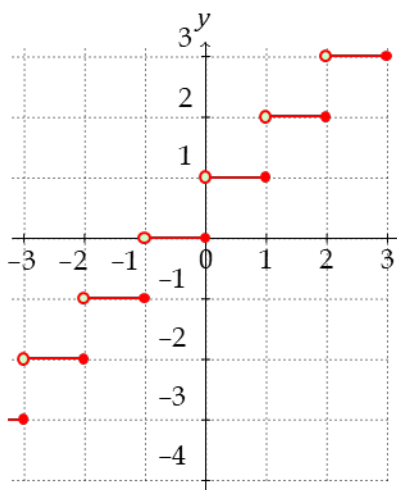
Since $(f \circ g)(x) = (f \circ g)(y)$, from the definition of composition of functions we have that $f(g(x)) = f(g(y))$. Since f is one-to-one, we conclude $g(x) = g(y)$. Then since g is one-to-one, we get $x = y$. ■

Chapter 12 Solutions:

Exercise 12.1. *Complete the definition of $\lceil x \rceil$.*

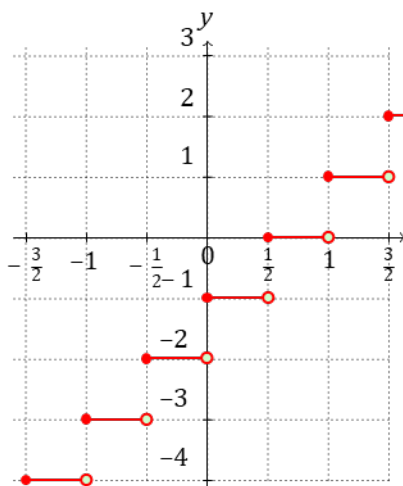
$\lceil x \rceil$ is the smallest integer that is greater than or equal to x .

Exercise 12.2. *Draw a college algebra graph of $f(x) = \lceil x \rceil$.*



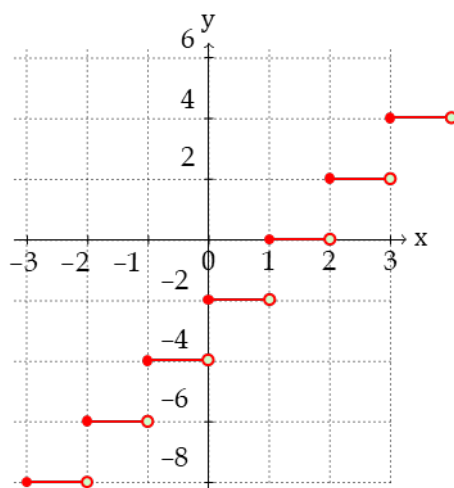
Exercise 12.3. Draw a college algebra graph of $f(x) = \lfloor 2x - 1 \rfloor$.

We could fall back on the plot-a-billion-points method of graphing, but it is a better idea to think first. Since we have a composition involving the floor function, there will be a jump by 1 at every integer input. That is, when $n = 2x - 1$ is an integer, there will be a jump up by 1 in the graph. If we solve for x we see that this means $x = (n + 1)/2$ where n is an integer. So the graph will jump at $-2 = -\frac{4}{2}, -\frac{3}{2}, -1 = -\frac{2}{2}, -\frac{1}{2}, 0, \frac{1}{2}, 1 = \frac{2}{2}, \dots$. Moreover the jump at the value $x = (n + 1)/2$ will be from $n - 1$ to n .



Exercise 12.4. Draw a college algebra graph of $f(x) = 2\lfloor x - 1 \rfloor$.

The graph of $y = \lfloor x - 1 \rfloor$ will be shift one unit to the right of the graph of $y = \lfloor x \rfloor$. So the graph of $f(x) = 2\lfloor x - 1 \rfloor$ will simply be the graph of $y = \lfloor x - 1 \rfloor$ with the outputs scaled by a factor of 2.



Exercise 12.5. Where does one function catch up with another?

The functions $f(x) = 18x$ and $g(x) = x^3/2$ cross when $18x = \frac{x^3}{2}$. That is, when

$$36x = x^3$$

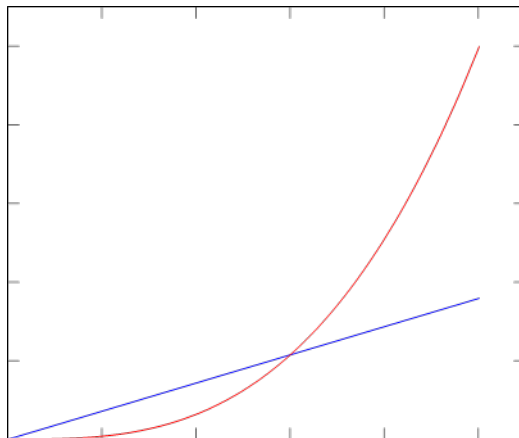
$$x^3 - 36x = 0$$

$$x(x^2 - 36) = 0$$

$$x(x - 6)(x + 6) = 0$$

$$x = -6, 0, 6$$

as seen in the graph. So, for $x > 0$, g catches f at $x = 6$.



Exercise 12.6. *Does one function catch up with another or stay behind?*

The exponential function $g(x) = 2^x$ ultimately dominates the power function $f(x) = 4x^5$. To see that, let's find a number $x > 1$ so that $\ln(2^x) > \ln(4x^5)$. That inequality can be rewritten as $x \ln 2 > \ln 4 + 5 \ln x$. Since all we care about is showing there is an x for which that inequality is true, we can make some simplifying substitutions: if $x/2 > 2 + 5 \ln x$, that would guarantee $x \ln 2 > \ln 4 + 5 \ln x$ because $x \ln 2 > x/2$. So, let's see if we can find x with $x > 4 + 10 \ln x$ and since we can make x as large as we want, we can also guarantee $\ln x \geq 4$. Consequently, we need only be sure we can pick x with $x > 11 \ln x$. Thinking about the graph of $y = x$ and the graph of $y = 11 \ln x$, we can see there will certainly be such an x . If we know a bit of calculus, we can compute slopes of tangent lines to the two curves to show there is such an x . If we have a computer algebra system, we can find a specific value of such an x . In fact, it turns out that 41 is the smallest integer greater than 1 for which $x > 11 \ln x$.

Exercise 12.7. *How can you compute $2^{\sqrt{2}}$ if your calculator's x^y button is broken?*

Assuming your other buttons work, use the fact that $\log(2^{\sqrt{2}}) = \sqrt{2} \log 2$. Here are the steps

- Compute $\sqrt{2} \cong 1.41421 \dots$
- Multiply by $\log 2 \cong 0.42572 \dots$
- Take the inverse log (10^x button if using base 10 logarithms) $2^{\sqrt{2}} \cong 2.66514 \dots$

Chapter 13 Solutions:

Exercise 13.1. *Guess the next term in a sequence.*

A great source of information about numerical sequences is *The Online Encyclopedia of Integer Sequences* at <http://oeis.org>. The search function on the site finds over 200 sequences that either begin or are otherwise related to 1, 2, 4, 5, 7, 8.

One possible answer: It looks like the list of positive integers in order, skipping the multiples of 3. So, the next few terms will be 10, 11, 13, 14, 16, 17.

Another answer: The positive integers n (in increasing order) for which $2n + 3$ is a prime. The next few terms would be 10, 13, 14, 17, 19, 20.

Exercise 13.2. *Give the 100th term of an arithmetic sequence.*

$a_{100} = 2 + 6 \cdot 99 = 596$ where the initial term is 2 and the common difference is 6.

Exercise 13.3. *Given the 10th and 16th terms of an arithmetic sequence, find the 11th.*

Let a be the initial term and d the common difference. Then we have that $a + 9d = -4$ from the 10th term and $a + 15d = 47$ from the 16th term. Subtract the 1st equation from the 2nd equation to get $6d = 51$. Thus $d = \frac{51}{6} = \frac{17}{2}$. From the 1st equation $a = -4 - 9d = -4 - 9 \cdot \frac{17}{2} = -161/2$.

That means that the 11th term is $-\frac{161}{2} + 10 \cdot \frac{17}{2} = \frac{9}{2}$.

Exercise 13.4. *Given the common ratio and initial term give the 5th term of a geometric sequence.*

$g_5 = 6 \cdot 2^4 = 6 \cdot 16 = 96$ since the initial term is $g_1 = 6$ and the common ratio is 2.

Exercise 13.5. *Given two consecutive terms of a geometric sequence, what is g_5 ?*

If r is the common ratio, then $g_2 = -11 = g_1 r = 5r$ so $r = -11/5$. That means that the 5th term is $g_5 = g_1 r^4 = 5 \cdot \left(-\frac{11}{5}\right)^4 = \frac{14641}{125}$.

Exercise 13.6. *Which sequences are both geometric and arithmetic?*

Suppose we have a sequence with initial term a that is arithmetic with common difference d as well as geometric with common ratio r . For the 2nd and 3rd terms in the sequence the formulas for the arithmetic sequence and geometric sequence must coincide so, we get $a + d = ar$ and also $a + 2d = ar^2$. The first equation tells us that $d = a(r - 1)$. Subtracting the 1st equation from the 2nd equation gives $d = ar^2 - ar = ar(r - 1)$. So $a(r - 1) = ar(r - 1)$. This equation leaves only a few options for a and r . 1) It could be that $a = 0$ in which case $d = 0$ and the sequence is 0, 0, 0, 0, ..., or 2) $r - 1 = 0$, so $r = 1$, and that means $d = 0$, and the sequence is $a, a, a, a, \dots$, or 3) $a \neq 0$ and $r - 1 \neq 0$ in which case $a(r - 1) = ar(r - 1)$ reduces to $r = 1$ which can't be in this case. Conclusion: the constant sequences $a, a, a, a, \dots$ are the only sequences that are both arithmetic (initial term a and common difference 0) and geometric (initial term a and common ratio 1).

Exercise 13.7. *Evaluate a sum.*

$$\sum_{j=1}^4 (j^2 + 1) = 2 + 5 + 10 + 17 = 34.$$

Exercise 13.8. *Evaluate a sum.*

$$\sum_{k=-2}^4 (2k - 3) = -7 - 5 - 3 - 1 + 1 + 3 + 5 = -7.$$

Exercise 13.9. *Find the sum of the first 100 terms of an arithmetic sequence.*

The initial term is 2, the 100th term is $2 + 6 \cdot 99$ so the total is $100 \left(\frac{2+2+6 \cdot 99}{2} \right) = 29900$.

Exercise 13.10. *Find the sum of the first five terms of a geometric sequence.*

$$6 + 12 + 24 + 48 + 96 = 186.$$

Exercise 13.11. *Evaluate a geometric sum.*

$$1 - \frac{3}{2} + \frac{9}{4} - \frac{27}{8} + \frac{81}{16} = \frac{55}{16}.$$

Exercise 13.12. *Express a sum in summation notation.*

$$\sum_{k=1}^n \frac{1}{2k}.$$

Chapter 14 Solutions:

Exercise 14.1. *List the first five terms of a recursively defined sequence.*

$$3, 15, 255, 65535, 42949667295.$$

Exercise 14.2. *List the first seven terms of a recursively defined sequence.*

$$1, 1, 2, 3, 7, 22, 155.$$

Exercise 14.3. *List the first ten terms of a recursively defined sequence.*

$$1, 2, 3, 3, 4, 4, 4, 4, 5, 5.$$

Exercise 14.4. *List the first ten terms of a recursively defined sequence and guess a closed form.*

1, 0, 3, 2, 5, 4, 7, 6, 9, 8. It looks like the terms alternately give one more and one less than the term index. That suggests that $a_n = n + (-1)^n$, for $n \geq 0$.

Exercise 14.5. Given the first few terms of a sequence use recursive thinking to guess the next term.

This is the *Look-and-Say* sequence introduced by John Horton Conway. After the initial term equal to 1, each new term is produced by *reading* the previous term. So for example:

- The second term is “one 1” from reading 1 and is written 11.
- The next term is read as “two 1” from reading 11 and is written 21.
- The next term reads “one 2 and one 1” and is written 1211.
- The next term reads “one 1, one 2 and two 1” and is written 111221, etc.

The term following 1113213211 is 31131211131221

Exercise 14.6. Give a recursive definition of the sum of n d's.

For $n = 1$ we define $1 \cdot d = d$. For the recursive part, for $n > 1$ we define $nd = (n - 1)d + d$.

Chapter 15 Solutions:

Exercise 15.1. *Given a recursive definition of a set, find the set.*

S is the set of positive integers.

Exercise 15.2. Give a recursive definition of a set.

Initial: $17 \in S$. Recursive: If $n \in S$, then $n + 100 \in S$.

Exercise 15.3. Give a recursive definition of a set.

Initial: $1, 2, 3 \in S$. Recursive: If $n \in S$, then $n + 4 \in S$.

Exercise 15.4. *Given a recursive definition of a set, describe the set.*

Each string in S consists of zero or more a 's followed on the right by an equal number of the two-letter combination bc . Examples $aabcbcb$ and $aaaabcbcbcbcbcbcb$. In exponential notation we might write $S = \{a^k(bc)^k | k \in \mathbb{N}\}$.

Exercise 15.5. *Given a recursive definition of a set, describe the set.*

The strings in S consist of one or more c 's preceded on the left by any combination of zero or more a 's and b 's. Examples $cccc, abbbac, babbacc, aaacc$. In exponential notation we might write $S = \{xc^k | x \in T, k \in \mathbb{Z}^+\}$ where $T = T_0 \cup T_1 \cup \dots \cup T_n \cup \dots$ and $T_m = \{a, b\}^m$.

Exercise 15.6. Given a recursive definition of the set of palindromes over $\Sigma = \{a, b, c\}$.

Initial: $\lambda, a, b, c \in S$. Recursive: If $x \in S$, then $axa, bxb, cxc \in S$.

Or Initial: $\lambda, a, b, c \in S$. Recursive: If $x, y \in S$, then $xyx \in S$. Add a palindrome to both ends of a palindrome to get a longer palindrome.

Chapter 16 Solutions:

Exercise 16.1. Use induction to prove that for every integer $n \geq 1$, is

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}.$$

Proof. When $n = 1$ the left-hand side is $3 = 1 \cdot 3$ and the right-hand side is $\frac{1 \cdot 2 \cdot 9}{6} = 3$.

Inductive hypothesis: Suppose

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + k(k+2) = \frac{k(k+1)(2k+7)}{6} \text{ is true for some } k \geq 1.$$

Then by induction hypothesis:

$$\begin{aligned} 1 \cdot 3 + 2 \cdot 4 + \cdots + k(k+2) + (k+1)(k+3) &= \frac{k(k+1)(2k+7)}{6} + (k+1)(k+3) \\ &= \frac{k(k+1)(2k+7)}{6} + \frac{6(k+1)(k+3)}{6} \\ &= \frac{(k+1)(k(2k+7) + 6(k+3))}{6} \\ &= \frac{(k+1)(2k^2 + 7k + 6k + 18)}{6} \\ &= \frac{(k+1)(2k^2 + 13k + 18)}{6} \\ &= \frac{(k+1)(k+2)(2k+9)}{6} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6} \quad \blacksquare \end{aligned}$$

Exercise 16.2. Prove that for every integer $n \geq 1$,

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2.$$

Proof. When $n = 1$, the left-hand side is $1 \cdot 2^1 = 2$ and $(1-1)2^{1+1} + 2 = 2$ too.

Inductive hypothesis: Suppose

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + k2^k = (k-1)2^{k+1} + 2 \text{ is true for some } k \geq 1.$$

Then by induction hypothesis:

$$\begin{aligned} 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + k2^k + (k+1)2^{k+1} &= (k-1)2^{k+1} + 2 + (k+1)2^{k+1} \\ &= [(k-1) + (k+1)]2^{k+1} + 2 \\ &= 2k2^{k+1} + 2 \\ &= ((k+1)-1)2^{k+2} + 2. \quad \blacksquare \end{aligned}$$

Exercise 16.3. The Fibonacci sequence is defined recursively by $f_0 = 0$, $f_1 = 1$, and, for $n \geq 2$, $f_n = f_{n-1} + f_{n-2}$. Use induction to prove that for all $n \geq 0$, $f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$.

Proof. When $n = 0$, $0 = f_0 = 1 - 1 = f_2 - 1$. So the base case is correct.

Inductive hypothesis: Suppose $f_0 + f_1 + f_2 + \cdots + f_k = f_{k+2} - 1$ for some $k \geq 0$.

By inductive hypothesis $f_0 + f_1 + f_2 + \cdots + f_k + f_{k+1} = f_{k+2} - 1 + f_{k+1}$.

$$\begin{aligned}
 &= (f_{k+1} + f_{k+2}) - 1 \\
 &= f_{k+3} - 1, \text{ by the recursive formula.} \\
 &= f_{(n+1)+2} - 1. \blacksquare
 \end{aligned}$$

Exercise 16.4. Prove by induction: For every integer $n > 4$, we have $2^n > n^2$.

Proof. When $n = 5$, the inequality is correct since $2^5 = 32 > 25 = 5^2$.

Inductive hypothesis: Suppose $2^k > k^2$ for some $k > 4$.

$(k + 1)^2 = k^2 + 2k + 1 < k^2 + 3k$ since $1 < 4 < k$.

$$\begin{aligned}
 &< k^2 + k \cdot k, \text{ since } 3 < 4 < k. \\
 &= 2k^2 < 2 \cdot 2^k, \text{ by inductive hypothesis.} \\
 &= 2^{k+1}. \blacksquare
 \end{aligned}$$

Exercise 16.5. Prove by induction: For every integer $n \geq 0$, $11^n - 6$ is divisible by 5.

Proof. When $n = 0$, $11^0 - 6 = 1 - 6 = -5$ is divisible by 5.

Inductive hypothesis: Suppose that $11^k - 6$ is divisible by 5 for some integer $k \geq 0$.

Then $11^{k+1} - 6 = 11 \cdot 11^k - 6 = 10 \cdot 11^k + (11^k - 6)$.

We are done because the sum of two multiples of 5 is a multiple of 5.

The first term on the right-hand side is $5(2 \cdot 11^k)$ and the second term on the right-hand side is a multiple of 5 by induction hypothesis. $\blacksquare$

Note: Here is another way to see that $11^n - 6$ is divisible by 5: for any integer $n \geq 0$, the number 11^n will have units digit 1, and so $11^n - 6$ will have units digit 5. Numbers with units digit 5 are divisible by 5. This proof does not answer the question posed however, since it is not a proof by induction.

Exercise 16.6. A pizza is cut into pieces (maybe some pretty oddly shaped) by making some integer $n \geq 0$ number of straight-line cuts. Prove: The maximum number of pieces is $(n^2 + n + 2)/2$.

Proof. When $n = 0$ there will be 0 cuts and therefore 1 piece. Luckily when $n = 0$, $\frac{n^2+n+2}{2} = 1$.

Inductive hypothesis: Suppose that for some $n \geq 0$, n straight lines cut produces a maximum number of $\frac{n^2+n+2}{2}$ pieces. Then

Inductive step: Suppose we add one more cut. Notice that when the new cut crosses an old cut, it will slice one old piece into two new pieces. We can't get more than two pieces when one cut crosses another since two straight lines cannot cross each other more than once. So, to get the maximum number of new pieces, we should make the new cut not parallel to the n previous cuts (and so, with care, be sure to cross all the previous cuts, and not at a point where previous cuts cross each other). This will give the maximum number of new pieces equal to $n + 1$. Conclusion: the maximum number of pieces with $n + 1$ straight cuts is

$$\frac{n^2 + n + 2}{2} + (n + 1) = \frac{n^2 + n + 2 + 2(n + 1)}{2} = \frac{(n + 1)^2 + (n + 1) + 2}{2}. \blacksquare$$

Exercise 16.7. A sequence is defined recursively by $a_0 = 0$, and, for $n \geq 1$, $a_n = 5a_{n-1} + 1$. Use induction to prove the closed form formula for a_n is

$$a_n = \frac{5^n - 1}{4}.$$

Proof. When $n = 0$ we are given $a_0 = 0$ and $(5^0 - 1)/4 = 0$. So the base case holds.

Inductive Hypothesis: Suppose that $a_k = (5^k - 1)/4$ for some integer $k \geq 0$.

Inductive Step: Then by using the recursive formula

$$\begin{aligned} a_{k+1} &= 5a_k + 1 \\ &= 5 \cdot \frac{5^k - 1}{4} + 1, \text{ by induction hypothesis.} \\ &= \frac{5^{k+1} - 5}{4} + \frac{4}{4} \\ &= \frac{5^{k+1} - 5 + 4}{4} \\ &= \frac{5^{k+1} - 1}{4}. \blacksquare \end{aligned}$$

Exercise 16.8. A sequence is defined recursively by $a_0 = 1$, $a_1 = 4$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$. Use induction to prove that the closed form formula for a_n is $a_n = 2 \cdot 3^n - 2^n$, $n \geq 0$.

Proof. Since the recursive formula uses the two previous terms we are going to have to check the formula for both a_0 and a_1 . They both work out fine since $a_0 = 1 = 2 \cdot 3^0 - 2^0$ and we also have when $a_1 = 4 = 2 \cdot 3^1 - 2^1$.

Inductive hypothesis: For $n \geq 2$ the term a_n depends on the two previous terms in the sequence, so we will use the second form of induction. Our hypothesis is that $a_k = 2 \cdot 3^k - 2^k$ for all k where $n \geq k \geq 0$ and $n \geq 1$ inclusive.

Inductive Step:

$$\begin{aligned}
a_{n+1} &= 5a_n - 6a_{n-1}, \text{ using the recursive formula since } n + 1 \geq 2. \\
&= 5(2 \cdot 3^n - 2^n) - 6(2 \cdot 3^{n-1} - 2^{n-1}), \text{ by the inductive hypothesis.} \\
&= (5 \cdot 2 \cdot 3 - 6 \cdot 2)3^{n-1} - (5 \cdot 2 - 6)2^{n-1}, \text{ regrouping and factoring} \\
&= 18 \cdot 3^{n-1} - 4 \cdot 2^{n-1} \\
&= 2 \cdot 3^2 \cdot 3^{n-1} - 2^2 2^{n-1} \\
&= 2 \cdot 3^{n+1} - 2^{n+1}, \text{ by the laws of exponents. } \blacksquare
\end{aligned}$$

Chapter 20 Solutions:

Exercise 20.1. Prove that if $a > 0$ and $b > 0$, then $ab > 0$.

Proof. Suppose $a > 0$ and $b > 0$. Since $a > 0$, multiplying both sides of $b > 0$ by a gives us $ab > a0$. We know $a0 = 0$ so we arrive at $ab > 0$. $\blacksquare$

Exercise 20.2. Prove that if $ab = 0$, then $a = 0$ or $b = 0$.

Proof. Suppose neither a nor b is 0. Consider four cases:

- a) $a > 0$ and $b > 0$: In this case, we proved $ab > 0$ in Exercise 20.1. Thus, $ab \neq 0$ in this case.
- b) $a > 0$ and $b < 0$: Since $a > 0$, multiplying both sides of $b < 0$ by a gives $ab < a0$. We know $a0 = 0$. It follows that $ab < 0$. So $ab \neq 0$ in this case.
- c) $a < 0$ and $b > 0$: Since $b > 0$, multiplying both sides of $a < 0$ by b gives $ab < b0$. We know $b0 = 0$. It follows that $ab < 0$. So $ab \neq 0$ in this case.
- d) $a < 0$ and $b < 0$: Since $a < 0$, multiplying both sides of $b < 0$ by a gives $ab > a0$. We know $a0 = 0$. It follows that $ab > 0$. In particular, $ab \neq 0$ in this case.

So, in any case, if neither a nor b is 0, then $ab \neq 0$. $\blacksquare$

Exercise 20.3. Prove the cancellation law for multiplication: For integers a, b, c , with $c \neq 0$, if $ac = bc$, then $a = b$.

Proof. Suppose $c \neq 0$ and $ac = bc$. We can rewrite $ac = bc$ as $ac - bc = 0$, and then use the distributive property to write that as $(a - b)c = 0$. Apply the result of Exercise 2 to conclude either $a - b = 0$ or $c = 0$. Since $c \neq 0$, it must be that $a - b = 0$. Adding b to each side of that equation shows $a = b$. $\blacksquare$

Chapter 21 Solutions:

Exercise 21.1. Determine the quotient and remainder when 107653 is divided by 22869.

$107563 = 4 \cdot 22869 + 16177$ so the quotient is 4 and the remainder is 16177.

Exercise 21.2. Determine if 1297 is a prime.

Since $36^2 = 1296 < 1297 < 37^2 = 1369$ it suffices to check to see if 1297 is divisible by any of the primes 2,3,5,7,11,13,17,19,23,29 and 31. None of these ten primes divides 1297 evenly, so 1297 is prime.

Exercise 21.3. Prove or give a counterexample: The divides relation is reflexive.

Proof. For any integer a we can write $a = a \cdot 1$. Therefore $\forall a \in \mathbb{Z}, a|a$. i.e. the divides relation is reflexive. ■

Exercise 21.4. Prove or give a counterexample: The divides relation is symmetric.

The divides relation is not symmetric. As a counterexample take $a = 2$ and $b = 4$. It is true that $2|4$, but $4|2$ is false.

Exercise 21.5. Prove or give a counterexample: The divides relation is transitive.

Proof. If $a|b$ and $b|c$, then there are integers k, l so that $b = ak$ and $c = bl$. By substitution we find $c = (ak)l = a(kl)$ where $kl \in \mathbb{Z}$. Thus $a|c$. ■

Exercise 21.6. What is wrong with the expression $4|12 = 3$?

The expression $4|12$ is a proposition. It is true since $12 = 4 \cdot 3$. So the correct notation would be $\frac{12}{4} = 3$.

Exercise 21.7. Show that none of the 1000 consecutive integers $1001! + 2$ to $1001! + 1001$ are primes.

Proof. The numbers are

$$1001! + 2, 1001! + 3, \dots, 1001! + k, \dots, 1001! + 1001.$$

The first number in the list is not a prime since 2 is a factor of each term, and so 2 is a factor of $1001! + 2$. Likewise, 3 is a proper factor of the second number, 4 is a proper factor on the third number, and so on, until 1001 is a proper factor of the 1000^{th} number in the list. So, none of the integers can be a prime. ■

Exercise 21.8. Prove: For $a, b \in \mathbb{Z}$, if $a|b$, then $-a|b$.

Proof. If $a|b$, then there is an integer k so that $b = ak$. But then $b = (-a)(-k)$ where $-k$ is an integer. Therefore, $-a|b$. ■

Chapter 22 Solutions:**Exercise 22.1.** *Use the Euclidean algorithm to compute $\gcd(a, b)$ in each case.*

a) $233 = 2 \cdot 89 + 55$

$89 = 1 \cdot 55 + 34$

$55 = 1 \cdot 34 + 21$

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$\gcd(233, 89) = 1$

b) $1001 = 77 \cdot 13 + 0$

$\gcd(1001, 13) = 13$

c) $2457 = 1 \cdot 1458 + 999$

$1458 = 1 \cdot 999 + 459$

$999 = 2 \cdot 459 + 81$

$459 = 5 \cdot 81 + 54$

$81 = 1 \cdot 54 + 27$

$54 = 2 \cdot 27 + 0$

$\gcd(2457, 1458) = 27$

d) $567 = 1 \cdot 349 + 218$

$349 = 1 \cdot 218 + 131$

$218 = 1 \cdot 131 + 87$

$131 = 1 \cdot 87 + 44$

$87 = 1 \cdot 44 + 43$

$$44 = 1 \cdot 43 + 1$$

$$43 = 43 \cdot 1 + 0$$

$$\gcd(567, 349) = 1$$

Exercise 22.2. Compute $\gcd(987654321, 123456789)$.

$$987654321 = 8 \cdot 123456789 + 9$$

$$123456789 = 13717421 \cdot 9 + 0$$

$$\gcd(987654321, 123456789) = 9$$

Exercise 22.3. Write a step-by-step algorithm that implements the Euclidean algorithm for finding greatest common divisors.

Here follows one solution:

Algorithm Euclidean Algorithm

Input: integers $m \geq 0, n > 0$

Output: $\gcd(m, n)$

1: $q \leftarrow m$	q represents a quotient
2: $r \leftarrow n$	r represents a remainder
3: while $r > 0$ do	
4: $g \leftarrow r$	Save the current r . It will be $\gcd(m, n)$ eventually.
5: $q = \lfloor m/n \rfloor$	Compute the new quotient
6: $q \leftarrow m - qn$	Compute the new remainder (becomes the next quotient)
7: $m \leftarrow n$	Update m
8: $n \leftarrow r$	Update n
8: end while	
9: output g	The last nonzero remainder.

Exercise 22.4. If n is a positive integer, what is $\gcd(n, 2n)$?

Since n divides both n and $2n$, it is a common divisor of n and $2n$. On the other hand, no integer larger than n can divide n . So, n is the largest common divisor of n and $2n$. So $\gcd(n, 2n) = n$.

Chapter 23 Solutions:

Exercise 23.1. Determine $\gcd(13447, 7667)$ and write it as a linear combination of 13447 and 7667. Try both the method of back-substitution and the Extended Euclidean Algorithm to determine a suitable linear combination.

$$13447 = 1 \cdot 7667 + 5780$$

$$7667 = 1 \cdot 5780 + 1887$$

$$5780 = 3 \cdot 1887 + 119$$

$$1887 = 15 \cdot 119 + 102$$

$$119 = 1 \cdot 102 + 17$$

$$102 = 6 \cdot 17 + 0$$

$$\gcd(13447, 7667) = 17$$

Part 1: Back-substitution:

$$17 = 1 \cdot 119 + (-1)102$$

$$= 1 \cdot 119 + (-1)(1887 + (-15)(119)) = 16 \cdot 119 + (-1)1887$$

$$= (-1)1887 + 16(5780 + (-3)1887) = 16 \cdot 5780 + (-49)1887$$

$$= 16 \cdot 5780 + (-49)(7667 + (-1)5780) = 65 \cdot 5780 + (-49)7667$$

$$= (-49)7667 + 65(13447 + (-1)7667) = 65 \cdot 13447 + (-114)7667$$

Part 2: Continued Fraction Table:

13447	7667	5780	1887	119	102	17	0
*	*	1	1	3	15	1	6
0	1	1	2	7	107	114	791
1	0	1	1	4	61	65	451
+	-	+	-	+	-	+	

Once again, we get $17 = 65 \cdot 13447 + (-114)7667$.

Exercise 23.2. What can you conclude about $\gcd(a, b)$ if $as + bt = 1$ for some integers s, t ?

Since 1 is a linear combination of a and b , we know that 1 is a multiple of $\gcd(a, b)$. Since greatest common divisors are positive, we must have $\gcd(a, b) = 1$.

Exercise 23.3. What can you conclude about $\gcd(a, b)$ if $as + bt = 19$ for some integers s, t ?

Since 19 is a linear combination of a and b , we know that 19 is a multiple of $\gcd(a, b)$. Since greatest common divisors are positive, we must have $\gcd(a, b) = 1$ or 19.

Exercise 23.4. *What can you conclude about $\gcd(a, b)$ if $as + bt = 18$ for some integers s, t ?*

Since 18 is a linear combination of a and b , we know that 18 is a multiple of $\gcd(a, b)$. Since greatest common divisors are positive, we must have $\gcd(a, b) = 1, 2, 3, 6, 9$ or 18.

Chapter 24 Solutions:

Exercise 24.1. *Determine the prime factorization of 345678.*

We try trial division by small primes (a calculator is not necessary initially)

$$345678 = 2 \cdot 172389 = 2 \cdot 3 \cdot 57613 = 2 \cdot 3 \cdot 17 \cdot 3389.$$

To test 3389 for primality we must check primes up to 53. Even this last part may be done without a calculator once we know some tricks from chapter 26.

Exercise 24.2. *Determine the prime factorization of 1016.*

$$1016 = 2 \cdot 508 = 2^2 \cdot 254 = 2^3 \cdot 127.$$

Remark: In each of the last two exercises every time we find a prime divisor the problem is reduced.

Exercise 24.3. *List all the positive divisors of 1016.*

All of the divisors of 1016 must be of the form $2^a 127^b$ where $a = 0, 1, 2, 3$ and $b = 0, 1$. Since there are four choices for a and two choices for b , there will be $4 \cdot 2 = 8$ distinct divisors:

$2^0 127^0 = 1$	$2^1 127^0 = 2$
$2^2 127^0 = 4$	$2^3 127^0 = 8$
$2^0 127^1 = 127$	$2^1 127^1 = 254$
$2^2 127^1 = 508$	$2^3 127^1 = 1016$

Exercise 24.4. *How many positive divisors does 345678 have?*

The positive divisors of 345678 will look like $2^a 3^b 17^c 3389^d$ where a, b, c, d can each be either 0 or 1. So, there will be a total of $2 \cdot 2 \cdot 2 \cdot 2 = 16$ positive divisors of 345678.

Chapter 25 Solutions:

Exercise 25.1. Find all integer solutions to $21x + 48y = 8$.

Since $\gcd(21,48) = 3$ and 3 does not divide 8 there are no integer solutions to this equation.

Exercise 25.2. Find all integer solutions to $21x + 48y = 9$.

Since $\gcd(21,48) = 3$ and 3 does divide 9 there are infinitely many integer solutions to this equation. Because the numbers are small we can find an initial solution by inspection

$$21 \cdot 5 + (-2)48 = 105 - 96 = 9, \text{ so } x = 5, y = -2.$$

Thus, all solutions are of the form

$$x = 5 + \frac{48}{\gcd(48,21)}k = 5 + 16k, y = -2 - \frac{21}{\gcd(21,48)}k = -2 - 7k, k \in \mathbb{Z}.$$

Or we could run the Extended Euclidean Algorithm:

$$48 = 2 \cdot 21 + 6$$

$$21 = 3 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

Back-substitution gives

$$3 = 1 \cdot 21 + (-3) \cdot 6 = 1 \cdot 21 + (-3)(48 + (-2)21) = 7 \cdot 21 + (-3)48$$

Multiplying through by 3 gives $9 = 3 \cdot 3 = 3(7 \cdot 21 + (-3)48) = 21 \cdot 21 + (-9)48$. In this case $x = 21$ and $y = -9$ (this solution is the case $k = 1$ from above. All solutions may be written in the form

$$x = 21 + 16m, y = -9 - 7m, m \in \mathbb{Z}.$$

Exercise 25.3. Find all integer solutions to $33x + 12y = 7$.

Since $\gcd(33,12) = 3$ and 3 does not divide 7 there are no integer solutions to this equation.

Exercise 25.4. Find all integer solutions to $33x + 12y = 6$.

Since $\gcd(33,12) = 3$ and 3 does divide 6 there are infinitely many integer solutions to this equation. By the Euclidean Algorithm and/or inspection $3 = 3 \cdot 12 + (-1) \cdot 33$. Multiply through by 2 to get the initial solution $x = -2, y = 6$ corresponding to $6 = (-2)33 + 6 \cdot 12$.

All solutions will be of the form

$$x = -2 + \frac{12}{\gcd(33,12)}k = -2 + 4k, y = 6 - \frac{33}{\gcd(12,33)}k = 6 - 11k, k \in \mathbb{Z}.$$

Exercise 25.5. *Sal sold some ceramic vases for \$59 each, and a number of bowls for \$37 each. If she took in a total of \$4270, how many of each item did she sell?*

First let's find all solutions to $59x + 37y = 4270$ by applying the Extended Euclidean Algorithm.

59	37	22	15	7	1	0
*	*	1	1	1	2	7
0	1	1	2	3	8	59
1	0	1	1	2	5	37
+	-	+	-	+	-	

The table shows $\gcd(59, 37) = 1 = (-5)59 + 8 \cdot 37$. Multiply through by 4270 to get an initial solution $4270 = 59 \cdot ((-5)4270) + 37 \cdot (8 \cdot 4270)$ so $x = (-5)4270, y = 8 \cdot 4270$ is one solution. All solutions are of the form

$$x = (-5)4270 + 37k, y = 8 \cdot 4270 - 59k, k \in \mathbb{Z}.$$

We need to find values of k where both $x, y \geq 0$. So we want to solve

$$(-5)4270 + 37k \geq 0 \quad \text{and} \quad 8 \cdot 4270 - 59k \geq 0.$$

The first inequality says $37k \geq 5 \cdot 4270$, so $k \geq \left\lceil \frac{5 \cdot 4270}{37} \right\rceil = 578$.

The second inequality says $8 \cdot 4270 \geq 59k$, so $\left\lfloor \frac{8 \cdot 4270}{59} \right\rfloor = 578 \geq k$.

Therefore, $k = 578, x = (-5)4270 + 37 \cdot 578 = 36$ and $y = 8 \cdot 4270 - 59 \cdot 578 = 58$.

Chapter 26 Solutions:

Exercise 26.1. *Answer the following timing questions:*

- a) *On a military (24-hour) clock, what time is it 3122 hours after 16 hundred hours?*

Taking 0 hours as midnight, the time 3122 hours after 16 hundred hours is going to be $16 + 3122 \equiv 3138 \equiv 18 \pmod{24}$. So, it's going to be 6 p.m. or 1800 hours.

- b) *What day of the week is it 3122 days after a Monday?*

Taking Sunday as day 0 of the week, the day 3122 days after Monday is going to satisfy $1 + 3122 \equiv 3123 \equiv 1 \pmod{7}$. So, it's going to be Monday.

- c) *What month is it 3122 months after November?*

Taking January as month 1, the month 3122 months after November is going to satisfy $11 + 3122 \equiv 3133 \equiv 1 \pmod{12}$. So, it's going to be January.

Exercise 26.2. *List the integers in $[7]_{11}$.*

The integers in $[7]_{11}$ are given by adding any multiple of 11 to 7. So, 7, 18, 29, 40, 51, ... but also ... -26, -15, -4. More compactly all integers of the form $7 + 11k, k \in \mathbb{Z}$.

Exercise 26.3. *In a listing of the five equivalence classes modulo 5, four of the values are 1211, 218, -100 , and -3333 . What are the possible choices for the fifth value?*

We compute $1211 \equiv 1 \pmod{5}$, $218 \equiv 3 \pmod{5}$, $-100 \equiv 0 \pmod{5}$ and $-3333 \equiv 2 \pmod{5}$. So, the missing equivalence class is $[4]_5$. Any member of the class will be a valid answer. These are integers of the form $4 + 5l$, $l \in \mathbb{Z}$. So, take your answer to be 4 or -1 or -6 etc.

Exercise 26.4. *Determine n between 0 and 24 such that $2311 + 3912 \equiv n \pmod{25}$.*

Reducing before adding is easier so

$$2311 + 3912 \equiv 11 + 12 \equiv 23 \pmod{25}$$

Exercise 26.5. *Determine n between 0 and 24 such that $2311 \cdot 3912 \equiv n \pmod{25}$.*

$$2311 \cdot 3912 \equiv 11 \cdot 12 \equiv 132 \equiv 7 \pmod{25}.$$

Exercise 26.6. *Determine n between 0 and 8 such that $1111^{2222} \equiv n \pmod{9}$.*

First, we can replace the base 1111 with $1 + 1 + 1 + 1 = 4$ by the casting 9's trick. So, instead of solving $1111^{2222} \equiv n \pmod{9}$ we are solving $4^{2222} \equiv n \pmod{9}$.

Next, we compute small powers of 4 modulo 9:

$$4^1 \equiv 4 \pmod{9}$$

$$4^2 \equiv 4 \cdot 4 \equiv 16 \equiv 7 \pmod{9}$$

$$4^3 \equiv 4 \cdot 4^2 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \pmod{9}$$

Thus $4^{3k} \equiv (4^3)^k \equiv 1^k \equiv 1 \pmod{9}$ for all integers k .

So $4^{2222} \equiv 4^{3 \cdot 740 + 2} \equiv (4^3)^{740} \cdot 4^2 \equiv 4^2 \equiv 16 \equiv 7 \pmod{9}$.

Exercise 26.7. *Solve: $4x \equiv 3 \pmod{7}$.*

Since $\gcd(4, 7) = 1$ and 1 divides 3, there will be exactly one solution to $4x \equiv 3 \pmod{7}$. Let's use trial-and-error to find that solution. Testing $x = 0, 1, 2, 3, 4, 5, 6$ we find

$$(4)(6) \equiv 24 \equiv 3 \pmod{7}.$$

So, the solution is $x \equiv 6 \pmod{7}$. Incidentally, it would be technically incorrect to say the solution is $x = 6$ since we are working modulo 7 and so the solution should be given modulo 7.

Alternatively, we can write $1 = 2 \cdot 4 + (-1) \cdot 7$ and multiply through by 3 to see that

$3 = 6 \cdot 4 + (-3) \cdot 7$ and arrive at the same conclusion.

Exercise 26.8. *Solve $11x \equiv 8 \pmod{57}$.*

The Extended Euclidean Algorithm lets us write $1 = (-5)57 + 26 \cdot 11$. Since 1 divides 8 we will have one solution, up to congruence: $x \equiv 26 \cdot 8 = 208 \equiv 37 \pmod{57}$.

Exercise 26.9. *Solve:* $14x \equiv 3 \pmod{231}$.

Since $\gcd(14, 231) = 7$ and 7 does not divide 3, this congruence has no solutions.

Exercise 26.10. *Solve* $8x \equiv 16 \pmod{28}$.

The Extended Euclidean Algorithm lets us write $4 = (-1)28 + 4 \cdot 8$. Since 4 divides 16 we will have four solutions up to congruence: $x_0 \equiv 4 \cdot 4 \equiv 16 \pmod{28}$, $x_1 = x_0 + \frac{28}{4} = 23$, and also $x_2 \equiv 16 + 2 \cdot 7 \equiv 30 \equiv 2 \pmod{7}$ and $x_3 \equiv 16 + 3 \cdot 7 \equiv 37 \equiv 9 \pmod{7}$.

Alternatively, we can divide the congruence through by 4 to obtain $2x \equiv 4 \pmod{7}$ which has the solution $x \equiv 2 \pmod{7}$. But since we seek solutions to $8x \equiv 16 \pmod{28}$ we must list the classes modulo 28 that are congruent to 2 modulo 7. Which gives the same congruence classes as solutions.

Exercise 26.11. *Solve:* $91x \equiv 189 \pmod{231}$.

The Extended Euclidean Algorithm lets us write $7 = (-5)91 + 2 \cdot 231$. Since 7 divides 189 we will have seven solutions up to congruence. An initial solution is

$$x_0 \equiv (-5) \cdot 27 \equiv -135 \equiv 96 \pmod{231}.$$

The other solutions differ by multiples of $231/7 = 33$. So we wind up with

$$x \equiv 30, 63, 96, 129, 162, 195 \text{ or } 228 \pmod{231}.$$

We could also solve $13x \equiv 27 \pmod{33}$ and rewrite as solutions mod 231 as in exercise 26.10.

Chapter 27 Solutions:

Exercise 27.1. *Convert to decimal:* 21_3 , 321_4 , 4321_5 , and FED_{16} .

Using Horner's Algorithm:

$$2 \mapsto 2 \cdot 3 + 1 = 7, \text{ so } 21_3 = 7.$$

$$3 \mapsto 3 \cdot 4 + 2 = 14 \mapsto 14 \cdot 4 + 1 = 57, \text{ so } 321_4 = 57.$$

$$4 \mapsto 4 \cdot 5 + 3 = 23 \mapsto 23 \cdot 5 + 2 = 117 \mapsto 117 \cdot 5 + 1 = 586, \text{ so } 4321_5 = 586.$$

$$F = 15 \mapsto 15 \cdot 16 + 14 = 254 \mapsto 254 \cdot 16 + 13 = 4077, \text{ so } FED_{16} = 4077.$$

Exercise 27.2. *Convert the decimal integer 11714 to bases 2, 6, and 16. Remember to use A to F to represent base 16 digits from 10 to 15, if needed.*

By the reverse of Horner's Method $11714 = 10110111000010_2 = 130122_6 = 2DC2_{16}$.

Exercise 27.3. Complete the following base 7 multiplication table.

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

Exercise 27.4. Make base 6 addition and multiplication tables similar to the base 7 multiplication table of exercise [27.3](#).

+	1	2	3	4	5
1	2	3	4	5	10
2	3	4	5	10	11
3	4	5	10	11	12
4	5	10	11	12	13
5	10	11	12	13	14

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	10	12	14
3	3	10	13	20	23
4	4	12	20	24	32
5	5	14	23	32	41

Exercise 27.5. (For those with a sweet tooth for punishment!) Use the Euclidean algorithm to compute $\gcd(5122_7, 1312_7)$ without converting the numbers to base 10.

Using the base 7 multiplication table above and omitting the subscript:

$$5122 = 3 \cdot 1312 + 553$$

$$1312 = 1 \cdot 553 + 426$$

$$553 = 1 \cdot 426 + 124$$

$$426 = 3 \cdot 124 + 21$$

$$124 = 4 \cdot 21 + 10$$

$$21 = 2 \cdot 10 + 1$$

$$10 = 10 \cdot 1 + 0$$

$$\gcd(5122_7, 1312_7) = 1_7.$$

Chapter 28 Solutions:

Exercise 28.1. *To meet the science requirement a student must take one of the following courses: a choice of 5 biology courses, 4 physics courses, or 6 chemistry courses. In how many ways can one course be selected?*

The key word being or, the number of options for one course is $5 + 4 + 6 = 15$.

Exercise 28.2. *Using the data of problem 1, a student has decided to take one biology, one physics, and one chemistry course. How many different such selections are possible?*

The number of options for a program of three courses is $5 \cdot 4 \cdot 6 = 120$.

Exercise 28.3. *A serial code is formed in one of three ways: (1) two letters followed by two digits, or (2) three letters followed by one digit, or (3) four letters. How many different codes are there? (Unless otherwise indicated, letters will mean upper case letters chosen from the usual 26-letter alphabet and digits are selected from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.)*

By the multiplication principle there are $26^2 \cdot 10^2$ codes of the first type, $26^3 \cdot 10^1$ codes of the second type and $26^4 \cdot 10^0$ codes of the third type. Since the types are disjoint the total number of codes is $26^2 \cdot 10^2 + 26^3 \cdot 10 + 26^4$ by the addition principle.

Exercise 28.4. *How many words of length six are there if letters may be repeated? (Examples: BBBXBB, ABATBC are OK).*

Assuming we are only using uppercase English letters the answer is 26^6 by the multiplication principle. But if we mean both uppercase and lowercase letters the answer is 52^6 .

Exercise 28.5. *How many words of length six are there if letters may not be repeated? (Examples: BBBBXX, ABATJC are bad but ABXHYP is OK).*

Assume only uppercase letters are used. The answer is $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21$.

Exercise 28.6. *A true/false test contains 25 questions.*

a) *How many ways can a student complete the test if every question must be answered?*

2^{25} (there are two choices for each answer, T or F).

b) *How many ways can a student complete the test if questions can be left unanswered?*

3^{25} (there are three choices for each answer, T, F or blank).

Exercise 28.7. *How many binary strings of length less than or equal to nine are there?*

By the multiplication principle there are 2^k bit strings of length $k \geq 0$. So by the addition principle the answer is $1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 = 2^{10} - 1 = 1023$.

Exercise 28.8. *How many eight-letter words contain at least one A?*

Assume only uppercase letters are used. The total number of eight letter strings over the alphabet is 26^8 . There are 25^8 of these with no A's. So, the answer is $26^8 - 25^8$.

Exercise 28.9. *How many seven-letter words contain at most one A?*

The number of seven-letter words with no A's is 25^7 . The number of seven-letter words with exactly one A is $7 \cdot 25^6$ (the seven reflects the number of spots the A can be in). By the addition principle the total is $25^7 + 7 \cdot 25^6$.

Exercise 28.10. *How many nine-letter words contain at least two A's?*

The number of nine-letter words with at least two A's is the total number of nine-letter words, minus the number of nine-letter words that contain at most one A. So, by the exclusion principle the answer is $26^9 - (25^9 + 9 \cdot 25^8)$.

Chapter 29 Solutions:

Exercise 29.1. *In how many ways can the 26 volumes (labeled A through Z) of the Encyclopedia of Pseudo-Science be placed on a shelf?*

$$26! = 403,291,461,126,605,635,584,000,000$$

Exercise 29.2. *In how many ways can those same 26 volumes be placed on a shelf if superstitions demand the volumes labeled with vowels must be adjacent? In how many ways can they be placed on the shelf obeying the conflicting superstition that volumes labeled with vowels cannot touch each other?*

Part 1: Assume that the vowels are a, e, i, o, u . First order the vowels, $5!$ ways. And then order the consonants, $21!$ ways. Think of the vowels as one big volume and place it somewhere in the order of the consonants 22 ways to do that. Final answer $5! \cdot 22!$.

Part 2: Assume that the vowels are a, e, i, o, u . First order the vowels, $5!$ ways. And then order the consonants, $21!$ ways. Now choose 5 spots before, or in between the consonants to place the vowels to keep them separate $C(22,5)$ ways. The total is thus $5! 21! C(22,5)$.

Exercise 29.3. *For those same 26 volumes, how many ways can they be placed in a two-shelf bookcase if volumes A-M go on the top shelf and N-Z go on the bottom shelf?*

There are $13!$ ways to arrange each shelf. So the total is $(13!)(13!) = (13!)^2$.

Exercise 29.4. *In how many ways can seven men and four women sit in a row if the men must sit together?*

This is the vowel consonant problem as in exercise 29.2 part 1. Answer $7! \cdot 4! \cdot 5 = 7! \cdot 5!$.

Exercise 29.5. 20 players are to be divided into two 10 –person teams. In how many ways can that be done?

We need to select 10 of the 20 to form one of the teams (the remaining 10 will form the other team). That can be done in $C(20,10)$ ways. If the teams have names (are distinguishable) we are done. Otherwise, this is a perfect double count. So, the final answer is $\frac{1}{2}C(20,10)$.

Exercise 29.6. A lottery ticket consists of five different integers selected from 1 to 99. How many different lottery tickets are possible? How many tickets would you need to buy to have a one-in-a-million chance of winning by matching all five randomly selected numbers?

The order of the numbers on the lottery ticket do not matter. Thus there are $C(99,6)$ possible lottery tickets. In order to have at least a one-in-a-million chance of winning the lottery by matching all five numbers we need to buy n tickets where $n/C(99,6) \geq 1/1,000,000$. That means that $n \geq C(99,6)/1,000,000 = 71,523,144/1,000,000 = 71.523144$. That means we have to buy at least 72 tickets.

Exercise 29.7. A committee of size six is selected from a group of nine deans and thirteen professors.

(a) How many different committees are possible?

We need a 6 –subset of the $9 + 13 = 22$ people. There are $C(22,6)$ of those.

(b) How many committees are possible if there must be exactly two deans on the committee?

First select two deans. There are $C(9,2)$ ways to do that.

Next select four professors: There are $C(13,4)$ ways to do that.

By the multiplication principle the final answer is $C(9,2) \cdot C(13,4)$.

(c) How many committees are possible if professors must outnumber deans on the committee?

The options are six professors and no deans, or five professors and one dean, or four professors and two deans. The total number of acceptable committees is

$$\binom{13}{6}\binom{9}{0} + \binom{13}{5}\binom{9}{1} + \binom{13}{4}\binom{9}{2}.$$

Chapter 30 Solutions:

Exercise 30.1. Determine the sixth row of Pascal's Triangle.

Given that the fifth row is 1 5 10 10 5 1 we can use Pascal's Identity to obtain the sixth row by starting and end with 1's and filling in the sums of consecutive terms of the 5th row.

$$\begin{array}{cccccccc} 1 & 1+5=6 & 5+10=15 & 10+10=20 & 10+5=15 & 5+1=6 & 1 \\ & 1 & 6 & 15 & 20 & 15 & 6 & 1 \end{array}$$

Exercise 30.2. Determine the coefficient of x^3y^7 in the expansion of $(3x - 2y)^{10}$.

$$\binom{10}{3} 3^3 (-2)^7 = -414270.$$

Exercise 30.3. Give an algebraic proof that

$$\binom{2n}{2} = 2 \binom{n}{2} + n^2.$$

Proof. We have

$$\begin{aligned} \binom{2n}{2} &= \frac{2n!}{2! (2n-2)!} = \frac{(2n)(2n-1)[(2n-2)!]}{2! (2n-2)!} = \frac{2n(2n-1)}{2} = n(2n-1) = 2n^2 - n \\ &= n^2 - n + n^2 = 2 \left(\frac{n(n-1)}{2} \right) + n^2 = 2 \left(\frac{n(n-1)[(n-2)!]}{2! (n-2)!} \right) + n^2 \\ &= 2 \left(\frac{n!}{2! (n-2)!} \right) + n^2 = 2 \binom{n}{2} + n^2. \quad \blacksquare \end{aligned}$$

Exercise 30.4. Give an algebraic proof that

$$\binom{r}{s} \binom{s}{t} = \binom{r}{t} \binom{r-t}{s-t}.$$

Proof. We compute

$$\begin{aligned} \binom{r}{s} \binom{s}{t} &= \frac{r!}{s! (r-s)!} \cdot \frac{s!}{t! (s-t)!} = \frac{r!}{(r-s)! t! (s-t)!} = \frac{r! (r-t)!}{t! (r-t)! (s-t)! (r-s)!} \\ &= \frac{r!}{t! (r-t)!} \cdot \frac{(r-t)!}{(s-t)! [(r-t) - (s-t)]!} = \binom{r}{t} \binom{r-t}{s-t}. \quad \blacksquare \end{aligned}$$

Exercise 30.5. Give a combinatorial proof that

$$\binom{r}{s} \binom{s}{t} = \binom{r}{t} \binom{r-t}{s-t}.$$

Proof. Scenario: We want to pick a committee of s people from a company with r employees, and a subcommittee of t of those s to act as the committee's board. In how many ways can that be done?

Method 1: Select the s people from the total of all r ($\binom{r}{s}$ ways to do that), and then select t of those s to be the board ($\binom{s}{t}$ ways to do that). So according to the multiplication principle, there are $\binom{r}{s} \binom{s}{t}$ ways to form the committee and its board.

Method 2: First select the t people to serve on the board from the r people available ($\binom{r}{t}$ ways to do that). To fill out the committee, we need to pick $s - t$ more people from the remaining $r - t$

people ($\binom{r-t}{s-t}$ ways to do that). So, according to the multiplication principle, there are $\binom{r}{t}\binom{r-t}{s-t}$ ways to form the committee and its board.

Since the two counting methods must give the same answer, we get $\binom{r}{s}\binom{s}{t} = \binom{r}{t}\binom{r-t}{s-t}$. ■

Exercise 30.6. Using the same reasoning as in the combinatorial proof of the Binomial Theorem, determine the coefficient of $x^4y^5z^6$ in the expansion of $(x + y + z)^{15}$.

$(x + y + z)^{15} = (x + y + z)(x + y + z)(x + y + z) \dots (x + y + z)(x + y + z)$ where there are 15 of the trinomials $x + y + z$. When this is expanded, we will get a term of the form $x^4y^5z^6$ by selecting 4 of the 15 trinomials to take the x from, and then 5 of the remaining 11 trinomials to take the y from (and, by default, taking z from the remaining six trinomials). So the number of terms of the form $x^4y^5z^6$ (before terms are combined) will be

$$\binom{15}{4}\binom{11}{5}\binom{6}{6} = \frac{15!}{4!11!} \cdot \frac{11!}{5!6!} \cdot \frac{6!}{6!0!} = \frac{15!}{4!5!6!}.$$

Exercise 30.7. Show that if p is a prime and $0 < k < p$, then p divides $\binom{p}{k}$

Hint: When $\binom{p}{k}$ is written out, how many times does p occur as a factor of the numerator and how many times as a factor of the denominator?

Suppose that p is a prime and k is an integer with $1 < k < p$. By the binomial theorem and properties of integers the coefficient $C(p, k) = n$ is an integer. We rewrite $p! = n \cdot k! (p - k)!$.

Since p divides $p!$ it must divide $n \cdot k! (p - k)!$. So by Euclid's Lemma p must divide one of the factors. But if $1 < k < p$, then p cannot divide $k!$ since all of its prime factors are less than p . Similarly, every prime factor of $(p - k)!$ is less than p . So p cannot divide $(p - k)!$. Which means that p must divide n . ■

Chapter 31 Solutions:

Exercise 31.1. At a certain college no student is allowed more than two majors. How many students are in the college if there are 70 math majors, 160 chemistry majors, 230 biology majors, 56 geology majors, 24 physics majors, 35 anthropology majors, 12 double math-physics majors, 10 double math-chemistry majors, 4 double biology-math majors, 53 double biology-chemistry majors, 5 double biology-anthropology majors, and no other double majors?

Let M be the set of students with a math major, C : chemistry majors, B : biology majors, G : geology majors, P : physics majors, and A : anthropology majors. The total number of students is

$$491 = |M \cup C \cup B \cup G \cup P \cup A| = |M| + |C| + |B| + |G| + |P| + |A| - |M \cap P| - |M \cap C| - |M \cap B| - |B \cap C| - |B \cap A| = 70 + 160 + 230 + 56 + 24 + 35 - 12 - 10 - 4 - 53 - 5.$$

This takes advantage of the fact each student has at most two majors so that $|M \cap C \cap B| = 0$, $|M \cap C \cap P| = 0$ etc. Also some double majors have no students eg. $|M \cap A| = 0$.

Exercise 31.2. *How many bit strings of length 15 start with the string 1111, end with the string 1000 or have 4th through 7th bits 1010?*

Let A be the set of bit strings of length 15 that start with 1111 (they look like 1111 – – – – –). Let B be the set of bit strings of length 15 that end with 1000 (they look like – – – – –1000), and let C be the set of bit strings of length 15 with bits 4 through 7 equal to 1010 (they look like – – –1010 – – – – –). We need to compute $|A \cup B \cup C|$.

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 2^{11} + 2^{11} + 2^{11} - 2^7 - 2^8 - 2^7 + 2^4 = 5648. \end{aligned}$$

Exercise 31.3. *How many positive integers between 1000 and 9999 inclusive are divisible by any of 4, 10 or 25 (careful!)?*

Let A be the set of integers between 1000 and 9999 (inclusive) that are multiples of 4. To count the number of integers, n , in A , we want to solve $1000 \leq 4n \leq 9999$. In other words, solve the inequality $250 \leq n \leq 2499.75$. The number of integers in the interval $[250, 2499]$ is

$$2499 - 250 + 1 = 2250 = \lfloor 9000 \rfloor.$$

So $|A| = 2250$. Likewise, let B be the set of integers that are multiples of 10 in the range 1000 to 9999, we get $|B| = 900 = \lfloor 9000/10 \rfloor$. Lastly, let C being the set of integers that are multiples of 25 in that range, we get $|C| = 360$. Now things get a little trickier: For $A \cap B$ we want to count the integers that are both multiples of 4 and 10. But that is the same as the multiples of 20, so $|A \cap B| = 450 = \lfloor 9000/\text{lcm}(4,25) \rfloor$. Likewise, $A \cap C$ (multiples of 100) has $|A \cap C| = 90$, and $B \cap C$ (multiples of 50) has $|B \cap C| = 180$. Finally, $A \cap B \cap C$ (also multiples of 100) has $|A \cap B \cap C| = 90$. So

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 2250 + 900 + 360 - 450 - 100 - 180 + 100 = 2880. \end{aligned}$$

Exercise 31.4. *How many permutations of the digits 1, 2, 3, 4, 5, have at least one digit in its own spot? In other words, a 1 in the first spot, or a 2 in the second, etc. For example, 35241 is OK since it has a 4 in the fourth spot, and 14235 is OK, since it has a 1 in the first spot (and also a 5 in the fifth spot). But 31452 is no good. Hint: Let A_1 be the set of permutations that have 1 in the first spot, let A_2 be the set of permutations that 2 in the second spot, and so on.*

Letting A_1 be the set of permutations of 1, 2, 3, 4, 5 with 1 in spot 1, A_2 be the set of permutations of 1, 2, 3, 4, 5 with 2 in spot 2, and so on, until A_5 is the set of permutations of 1, 2, 3, 4, 5 with 5 in spot 5, we want to count in the number of elements in $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$.

All five of the counts $|A_1|, |A_2|, \dots, |A_5|$ will be be 4! (place one number in its spot, and arrange the other four in any way at all). Likewise, all ten counts like $|A_i \cap A_j|$ will be 3! (place two

numbers in the correct spots and arrange the remaining three in any way at all. Continuing, counts for $A_i \cap A_j \cap A_k$ type will be $2!$. For the $A_i \cap A_j \cap A_k \cap A_l$ type will be $1!$. Finally the number $|A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| = 0! = 1$ (every number is its correct spot). So,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5| &= 5 \cdot 4! - 10 \cdot 3! + 10 \cdot 2! - 5 \cdot 1! + 1 \\ &= 120 - 60 + 20 - 5 + 1 = 76. \end{aligned}$$

Exercise 31.5. *How many permutations of the digits 1, 2, 3, 4, 5 have no digit in its own spot?*

Using the exclusion principle, the number of permutations of 1, 2, 3, 4, 5 with no digit in its correct spot will be the total number of permutations of 1, 2, 3, 4, 5 minus the number of those permutations with at least one number in its correct spot. That is $5! - 76 = 120 - 76 = 44$. This is also writable as $5! - 5 \cdot 4! + 10 \cdot 3! - 10 \cdot 2! + 5 \cdot 1! - 0!$. By inductive reasoning you can solve the problem of **derangements** for a general positive integer n . A derangement of the integers 1 through n is a permutation of them in which no integer is in its original place.

Chapter 32 Solutions:

Exercise 32.1. *Show that in any group of eight people, at least two were born on the same day of the week.*

If we distribute eight objects (people) into seven piles (days of the week), there will be at least one pile (day) with $\lceil 8/7 \rceil = 2$ objects (people).

Exercise 32.2. *Show that in any group of 100 people, at least 15 were born on the same day of the week.*

If we distribute 100 objects (people) into seven piles (days of the week), there will be at least one pile (day) with $\lceil 100/7 \rceil = 15$ objects (people).

Exercise 32.3. *How many cards must be selected from a deck to be sure that at least six of the selected cards have the same suit?*

Since there are four suits (piles), we need the least value of n so that $\lceil n/4 \rceil = 6$. That means the smallest value of n will be $5 \cdot 4 + 1 = 21$.

Exercise 32.4. *Show that in any set of n integers, where $n \geq 2$, there must be a pair with a difference that is a multiple of $n - 1$.*

Let $a_1, a_2, \dots, a_n$ be n integers. They are each equivalent to one of $0, 1, 2, \dots, n - 2 \pmod{n - 1}$. Since there are n values, but only $n - 1$ options modulo $n - 1$, some two of those numbers must be the same modulo $n - 1$. Say $a_k \equiv a_j \pmod{n - 1}$. That means $n - 1$ divides $a_k - a_j$.

Exercise 32.5. *Al has 75 days to master discrete mathematics. He decides to study at least one hour every day, but no more than a total of 125 hours. Show there must be a sequence of consecutive days during which he studies exactly 24 hours.*

Let t_i denote the total number of hours studied from day 1 to day i . We are told

$$0 < t_1 < t_2 < \cdots < t_{75} \leq 125.$$

Add 24 to each of these numbers to get the chain of inequalities

$$24 < t_1 + 24 < t_2 + 24 < \cdots < t_{75} + 24 \leq 149.$$

So, we have 150 numbers (namely $t_1, t_2, \dots, t_{75}$ and $t_1 + 24, t_2 + 24, \dots, t_{75} + 24$) all between 1 and 149. By the Pigeonhole Principle some two of those must be equal. Since the numbers in the first list are all different, and the numbers in the second list are also all different, it must be that $t_i = t_j + 24$ for some i and j . That means $t_i - t_j = 24$.

That tells us that on days $j + 1, j + 2, \dots, i$, Al studied exactly a total of 24 hours.

Exercise 32.6. *Show that in any set of 217 integers, there must be a pair with a difference that is a multiple of 216.*

Since there are only 216 different values modulo 216, the pigeonhole principle says some two of the 217 numbers, say m and n , must have the same value modulo 216. So, $m \equiv n \pmod{216}$. That means $216 \mid (m - n)$. So, m and n have a difference that is a multiple of 216.

Chapter 33 Solutions:

Exercise 33.1. *How many quaternary strings of length n are there (a quaternary string uses 0's, 1's, 2's, and 3's)?*

There are four choices for each of the n positions, so there are 4^n quaternary strings of length n , where $n \geq 0$.

Exercise 33.2. *How many quaternary strings of length less than or equal to 7 are there?*

Including the empty string λ there are $1 + 4^1 + \cdots + 4^7 = \frac{4^8 - 1}{4 - 1} = \frac{4^8 - 1}{3} = 21,845$.

Exercise 33.3. *How many solutions in integers are there to*

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 54, \text{ where } 3 \leq x_1, 4 \leq x_2, 5 \leq x_3, \text{ and } 6 \leq x_4, x_5, x_6, x_7?$$

As a donut-shoppe problem, ask for 3 x'_1 's, 4 x'_2 's, 5 x'_3 's and half a dozen of each to the x'_4 's, x'_5 's, x'_6 's and x'_7 's. That gives 36 donuts ordered. Now order 18 more from among the 7 types. That means there are

$$\binom{18 + 7 - 1}{18} = \binom{24}{18} = 134,596 \text{ acceptable solutions to the equation.}$$

Exercise 33.4. *How many ternary strings of length n start 0101 and end 212?*

For ternary strings, each position is a 0, 1, or 2. If the ternary string begins 0101 and ends 212 (and must be of length 7 or more!). There will be $n - 7$ positions left to fill, and there are three choices for each position, so there are 3^{n-7} such strings (assuming $n \geq 7$).

Exercise 33.5. *A doughnut shop has 8 kinds of doughnuts: chocolate, glazed, sugar, cherry, straw- berry, vanilla, caramel, and jalapeño. How many ways are there to order three dozen doughnuts, if at least 4 are jalapeño, at least 6 are cherry, and at least 8 are strawberry, but there are no restrictions on the other varieties?*

When you build your order, tell the clerk to start with four jalapeño, six cherry, and eight strawberry. That accounts for 18 donuts, and so you need 18 more, and any combination is okay for those last 18. So, there are $\binom{8+18-1}{18} = \binom{25}{18} = 480,700$ ways to form the donut order.

Exercise 33.6. *How many strings of twelve lowercase English letters are there*

- a) which start and end with the letter x , if letters can be repeated?

26^{10} , since there are 26 choices for each spot.

- b) which contain the letter x exactly once, if letters can be repeated?

Pick a spot for the x (12 ways). Then fill in the string with non x 's 25^{11} ways. The final answer is $12 \cdot 25^{11}$ by the multiplication principle.

- c) which contain each of the letters x and y exactly once, if letters can be repeated?

Pick a spot for the x (12 ways). Pick a spot for the y (11 ways). Then, fill in the string with non x 's and non y 's 24^{10} ways. The final answer is $12 \cdot 11 \cdot 24^{10}$ by the multiplication principle.

- d) which contain at least one letter from the first half of the alphabet (a through m), where letters may be repeated?

There are 13 letters in the second half of the alphabet and so there are 13^{12} strings of 12 lowercase English letters which do not contain any letters from the first half of the alphabet. By the exclusion principle there are therefore $26^{12} - 13^{12}$ strings of twelve lowercase English letters that contain at least one letter from the first half of the alphabet.

Exercise 33.7. How many bit strings of length 19 either begin 0101, or have 4th, 5th and 6th digits 101, or end 1010?

Let A be the set of bit strings of length 19 of the form 0101 — — — — —.

Let B be the set of bit strings of length 19 of the form $---101-----$.

Let C be the set of bit strings of length 19 of the form $-----1010$.

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 2^{15} + 2^{16} + 2^{15} - 2^{13} - 2^{11} - 2^{12} + 2^9. \end{aligned}$$

Exercise 33.8. *How many pentary strings (i.e. strings using the digits 0,1,2,3,4) of length 15 consist of three 0's, four 1's, three 2's, four 3's and one 4?*

Task 1: Pick three of the fifteen spots for 0's: $\binom{15}{3}$ ways to do that.

Task 2: Pick four of the remaining twelve spots for 1's: $\binom{12}{4}$ ways.

Task 3: Pick three of the remaining eight spots for 2's: $\binom{8}{3}$ ways.

Task 4: Pick four of the remaining five spots for 3's: $\binom{5}{4}$ ways.

Task 5: Pick one of the remaining one spots for 4: $\binom{1}{1}$ ways.

By the multiplication principle the number of strings is

$$\binom{15}{3} \binom{12}{4} \binom{8}{3} \binom{5}{4} \binom{1}{1} = \frac{15!}{3! 12!} \cdot \frac{12!}{4! 8!} \cdot \frac{8!}{3! 5!} \cdot \frac{5!}{4! 1!} = \frac{15!}{3! 4! 3! 4! 1!} = 63,063,000$$

Exercise 33.9. *Seven lecturers and fourteen professors are on the faculty of a math department.*

- a) *How many ways are there to form a committee with seven members which contains more lecturers than professors?*

As usual, we assume people are distinguishable. We can pair 7, 6, 5 or 4 lecturers with 0, 1, 2 or 3 professors respectively.

$$\binom{7}{7} \binom{14}{0} + \binom{7}{6} \binom{14}{1} + \binom{7}{5} \binom{14}{2} + \binom{7}{4} \binom{14}{3}.$$

- b) *How many ways are there to form a committee with seven members where the professors outnumber the lecturers by at least a two-to-one margin?*

We can pair 7, 6, or 5 professors with 0, 1 or 2 lecturers respectively.

$$\binom{14}{7} \binom{7}{0} + \binom{14}{6} \binom{7}{1} + \binom{14}{5} \binom{7}{2}.$$

- c) *How many ways are there to form a committee with seven members consisting of at least five lecturers?*

The final size of the committee isn't specified so we will assume any size (five or more) is ok. We will pick 5, 6, or 7 lecturers and pair each selection with any subset of the professors.

$$\binom{7}{7} 2^{14} + \binom{7}{6} 2^{14} + \binom{7}{5} 2^{14}.$$

Exercise 33.10. *In how many ways can twenty people form a line at a ticket window if Hans and wife Brunhilda are having a spat, and refuse to stand in consecutive places in the line?*

There are $20!$ ways to form a line of the 20 people. If we tie Hans and Brunhilda together, there are 19 items, and so there are $19!$ ways to line those 19 items up. Of course, Hans and Brunhilda could be in either order, so there are $2(19!)$ bad lines. The number of lines is $20! - 2(19!)$.

Exercise 33.11. *Prove that a set with $n \geq 1$ elements has the same number of subsets with an even number of elements, as subsets with an odd number of elements.*

Proof: By induction we see that a set with one element has two subsets; $\emptyset$ and itself. The first has an even number of elements, the second has an odd number of elements.

Now suppose that for some $k \geq 1$ any set with k elements has the same number of subsets with even cardinality as subsets with odd cardinality.

Consider a set with $k + 1$ elements. In fact suppose that the set is the disjoint union of a set A with n elements and the set $\{e\}$, (e for extra element). List all of the subsets of A . By inductive hypothesis there will be some number t of subsets with even cardinality and an equal number t of subsets with odd cardinality. Adding the element e to each the t subsets of A with even cardinality will yield a previously unlisted subset of $A \cup \{e\}$ with odd cardinality. Likewise, adding the element e to each the t subsets of A with odd cardinality will yield a previously unlisted subset of $A \cup \{e\}$ with even cardinality. We conclude that $A \cup \{e\}$ has $2t$ subsets of even cardinality and $2t$ subsets of odd cardinality. ■

We remark that this is also the conclusion of Theorem 30.8.

Chapter 34 Solutions:

There are usually many different recursive formulas that will be correct answers to the problems below. If your answer does not agree with the answer provided, you should use both formulas to generate a number of terms, say six or eight or so. If the numbers do not agree, your work is wrong. If they do agree, then it is likely your work is okay. You could make sure of that by using induction, for example, to show the two recursive formulas are equivalent.

Exercise 34.1. *On day zero, a piggy bank contains \$0. Each day, one more penny is added to the bank than the day before. So, on day 1 one penny is added, on day 2 two pennies are added. Write a recursive formula for the total number of pennies in the bank each day, $n = 0, 1, 2, \dots$.*

Let p_n be the number of pennies in the bank on day n . The initial value is $p_0 = 0$. A recursive relation is $p_n = p_{n-1} + n$, for $n \geq 1$.

Exercise 34.2. *Al climbs stairs by taking either one or two steps at a time. For example, he can climb a flight of three steps in three different ways: (1) one step, one step, one step or (2) two step, one step, or (3) one step, two step. Determine a recursive formula for the number of different ways Al can climb a flight of n steps.*

For $n \geq 0$, let c_n be the number of different ways Al can climb n steps. The initial conditions are $c_0 = 1$, and $c_1 = 1$. For a recursive formula: When climbing $n \geq 2$ steps, Sal can start with one step and finish the climb in c_{n-1} ways or start with two steps and finish the climb in c_{n-2} ways. So, for $n \geq 2$, $c_n = c_{n-1} + c_{n-2}$.

Exercise 34.3. Find a recurrence relation for the number of bit strings of length n that contain an even number of 0's.

Let a_n be the number of bit strings of length n with an even number of 0's. For an initial condition, we have $a_1 = 1$ since the only good length 1 bit string is 1. If the empty bit string doesn't bother you, we could use initial condition $a_0 = 1$. Now we think recursively: If we have a good bit string of length $n - 1$, we can add a 1 to the end to get a good bit string of length n . That accounts for all the good length n bit strings that end with 1. We get the good bit strings of length n that end with 0 by adding 0 to the end of a *bad* length $n - 1$ bit string. Using the exclusion principle we see there are $2^{n-1} - a_{n-1}$ strings of length n of this type. So, one solution is $a_n = a_{n-1} + (2^{n-1} - a_{n-1}) = 2^{n-1}$, for $n \geq 1$. This fits a_1 , but not a_0 .

Exercise 34.4. Find a recurrence relation for the number of bit strings of length n that contain two consecutive 0's.

After computing $b_0 = 0$ and $b_1 = 0$, let's think about how to build length $n \geq 2$ good bit strings. We could add 00 to the right end of any of the 2^{n-2} bit strings of length $n - 2$. Or, we could add 10 to any of the b_{n-2} good bit strings of length $n - 2$. Or we could add 1 to any of the b_{n-1} good bit strings of length $n - 1$. These three options account for all the good length n bit strings, the first two count the length n bit strings that end with 0, and the last counts the good bit strings that end with 1. So, a recursive formula for the sequence is

$$b_n = b_{n-1} + b_{n-2} + 2^{n-2}, \text{ for } n \geq 2.$$

Exercise 34.5. Find a recurrence relation for the number of bit strings of length n that contain the string 01.

Let g_n be the number of good strings of length n , we get $g_0 = 0$, $g_1 = 0$, and $g_2 = 1$. Now let's think recursively. For good strings of length $n \geq 1$, we can make good strings of length $n + 1$ by adding a 0 to the right end, and that will account for all the good length $n + 1$ strings ending with a zero. Next, let's count the number of good length $n + 1$ strings ending with 1. Here there are several choices depending on the number of 1's that end the bit string (*any* will mean any bit string of appropriate length):

- (any)01 (2^{n-2} of these)
- (any)011 (2^{n-3} of these)
- (any) 0111 (2^{n-4} of these)
- $\vdots$
- and so on until we reach 01111 $\cdots$ 1 (1 of these).

By the addition principle we get

$$g_n = g_{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 = g_{n-1} + 2^{n-1} - 1, \text{ for } n \geq 1.$$

Exercise 34.6. Find a recurrence relation for the number of ternary strings of length n that contain two consecutive 0's.

Let A_k denote the set of ternary strings of length k with two adjacent 0's. Let $a_k = |A_k|$. We have $a_0 = 0 = a_1$ and $a_2 = 1$ by brute-force enumeration. Consider $x \in A_k$ for some $k \geq 2$. Either x starts with a 1, in which case $x = 1y$ where $y \in A_{k-1}$. Or x starts with a 2, in which case $x = 2y$ where $y \in A_{k-1}$. Or (exclusively) x starts with a 0. In this case the next bit in x must be 1 or 2 so $x = 01z$ where $z \in A_{k-2}$ or $x = 02z$ where $z \in A_{k-2}$. Finally if x starts 00 it can be followed by any ternary string of length $k - 2$. This covers all possibilities so by the addition principle

$$a_k = 2a_{k-1} + 2a_{k-2} + 3^{k-2}, \text{ for } k \geq 2 \text{ and } a_0 = 0 = a_1.$$

An alternative recursive answer (as given in sequence A186244 in the *The On-Line Encyclopedia of Integer Sequences*) (Google it!) is,

$$a_n = 3a_{n-1} + 2(3^{n-3} - a_{n-3}), \text{ for } n \geq 3 \text{ with } a_0 = 0 = a_1, a_2 = 1.$$

Reasoning: The recursive formula is based on adding any of 0, 1, 2 to strings of length $n - 1$ which already have 00 in them, or 100, 200 to strings of length $n - 3$ which do not.

Exercise 34.7. Find a recurrence relation for the number of subsets of $\{1, 2, 3, \dots, n\}$ that do not contain any consecutive integers. Examples for $n = 9$: the subset $\{1, 3, 8\}$ is good, but the subset $\{2, 5, 6, 9\}$ is bad since it contains the consecutive integers 5, 6.

Let $A_n = \{1, 2, 3, \dots, n\}$. A subset B of A_n is good if B does not contain any two consecutive integers. Let g_n be the number of good subsets of A_n . Split the good subsets of A_n into two groups: 1: Those subsets that contain n ; 2: those subsets that do not contain n .

Good subsets of type 1 cannot contain the element $n - 1$. So all of these subsets are formed by adding n to a good subset of A_{n-2} (where $n \geq 2$). Good subsets of type 2 are simply good subsets of A_{n-1} . Thus, by the addition principle, a recursive formula for $g_n = g_{n-1} + g_{n-2}$ as long as $n \geq 2$. The initial conditions are $g_0 = 1$ and $g_1 = 2$. This is a “shift” so to speak of the Fibonacci sequence.

Exercise 34.8. Suppose in the original Tower of Hanoi problem there are four clearings A, B, C, D . Find a recursive relation for J_n , the minimum number of moves needed to transfer the tower from clearing A to clearing D .

Surprisingly, this is a very difficult problem. A conjectured answer was given in 1941, and evidently the conjecture was proved correct in 2014. No one has been able to solve the problem for more than four pegs, though there are suspicions that remain unproven.

Chapter 35 Solutions:

Exercise 35.1. *Guess the solution to $a_0 = 2, a_1 = 4$ and for $n \geq 2, a_n = 4a_{n-1} - 3a_{n-2}$ and prove your guess is correct by induction.*

Using the given recursive formula we see the sequence begins 2, 4, 10, 28, 82, 244, and those values look a lot like powers of 3: 1, 3, 8, 27, 81, 243, so a good guess is $a_n = 3^n + 1$.

The base cases for the induction are $n = 0, 1$. We are given $a_0 = 2$ while $3^0 + 1 = 1 + 1 = 2$, and $a_1 = 4$ while $3^1 + 1 = 4$. So $a_n = 3^n + 1$ is correct for $n = 0, 1$. For the inductive step, suppose $a_k = 3^k + 1$ for all values of $k \leq n$ for some $n \geq 1$. Then

$$\begin{aligned} a_{n+1} &= 4a_n - 3a_{n-1} = 4(3^n + 1) - 3(3^{n-1} + 1) \\ &= 4 \cdot 3^n - 3^n + 4 - 3 = 3 \cdot 3^n + 1 = 3^{n+1} + 1. \blacksquare \end{aligned}$$

Exercise 35.2. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 5a_{n-1}$.*

$$a_n = 5a_{n-1} = 5(5a_{n-2}) = 5^2a_{n-2} = 5^2(5a_{n-3}) = 5^3a_{n-3}.$$

As we continue to unfold, eventually we will reach a_0 . Notice that the exponent on the 5 and the subscript on the a always add up to n . That makes sense since at each step the exponent goes up 1 and the subscript goes down 1, and so the exponent and the subscript always add up to the n they started at in the first step. That means we eventually reach $a_n = 5^n a_0$. Since $a_0 = 2$, we conclude $a_n = 2 \cdot 5^n$, for $n \geq 0$.

Exercise 35.3. *Solve by unfolding: $a_0 = 2$, and, for $n \geq 1, a_n = 5a_{n-1} + 3$. Hint: This one will involve applying the geometric sum formula.*

$$\begin{aligned} a_n &= 3 + 5a_{n-1} = 3 + 5(3 + 5a_{n-2}) \\ &= 3 + 5 \cdot 3 + 5^2a_{n-2} = 3 + 3 \cdot 5 + 5^2(3 + 5a_{n-3}) \\ &= 3 + 3 \cdot 5 + 3 \cdot 5^2 + 5^3a_{n-3} \end{aligned}$$

As we continue to unfold, the first group in parentheses will continue gaining one term at each step and the last term will have the exponent of the 5 going up one at a time while the subscript on the a will decrease by one at a time. Eventually we will reach the expression

$$\begin{aligned} a_n &= (3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^{n-1}) + 5^n a_0 \\ &= 3(1 + 5 + 5^2 + \cdots + 5^{n-1}) + 2 \cdot 5^n \\ &= 3 \frac{5^n - 1}{5 - 1} + 2 \cdot 5^n = \frac{11 \cdot 5^n - 3}{4}, \text{ for } n \geq 0. \end{aligned}$$

As a check of our work, we can use the recursive formula and the closed form formula to generate six or so terms to see if they produce the same values (or, if we are really ambitious, we can use induction to verify the closed form formula is correct). In any case, the recursive formula and the closed form formula both give 2, 13, 68, 343, 1718, 8593. So we can be confident that our work is correct.

Chapter 36 Solutions:

Exercise 36.1. For each of the following sequences find a recurrence relation satisfied by the sequence. Include a sufficient number of initial conditions to completely specify the sequence.

(a) $a_n = 2n + 3, n \geq 0$.

$a_0 = 3$ and for $n \geq 1, a_n = a_{n-1} + 2$.

But also $a_0 = 3, a_1 = 5$ and $a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 2$.

(b) $a_n = 3 \cdot 2^n, n \geq 1$.

$a_1 = 6$ and for $n \geq 2, a_n = 2a_{n-1}$.

(c) $a_n = n^2, n \geq 1$.

$a_1 = 1$ and for $n \geq 2, a_n = a_{n-1} + 2n - 1$.

Also $a_1 = 1, a_2 = 4, a_3 = 9$ and for $n \geq 3, a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3}$.

(d) $a_n = n + (-1)^n, n \geq 0$.

$a_0 = 1$ and for $n \geq 1, a_n = a_{n-1} + 2(-1)^n + 1$.

Also $a_0 = 1, a_1 = 0$ and for $n \geq 2, a_n = a_{n-2} + 2$.

Also $a_0 = 1, a_1 = 0, a_2 = 3$ and for $n \geq 3, a_n = a_{n-1} + a_{n-2} - a_{n-3}$.

To see the connection look at the factorizations of the characteristic polynomials

Solve each of the following recurrence relations:

Exercise 36.2. $a_0 = 3, a_1 = 6$ and $a_n = a_{n-1} + 6a_{n-2}$, for $n \geq 2$.

The characteristic equation is $\chi(x) = x^2 - x - 6 = (x + 2)(x - 3)$.

The characteristic roots are $x = -2, 3$.

The general solution is $a_n = \alpha(-2)^n + \beta \cdot 3^n$.

The initial values ($n = 0, 1$) produce the linear system of equations

$$\alpha + \beta = 3$$

$$-2\alpha + 3\beta = 6$$

The solution to this system is $\alpha = 3/5, \beta = 12/5$.

The closed form is $a_n = \frac{3}{5}(-2)^n + \frac{12}{5} \cdot 3^n$, for $n \geq 0$.

Exercise 36.3. $a_0 = 4, a_1 = 7$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$.

The characteristic equation is $\chi(x) = x^2 - 5x + 6 = (x - 2)(x - 3)$.

The characteristic roots are $x = 2, 3$.

The general solution is $a_n = \alpha \cdot 2^n + \beta \cdot 3^n$.

The initial values ($n = 0, 1$) produce the linear system of equations

$$\alpha + \beta = 4$$

$$2\alpha + 3\beta = 7$$

The solution to this system is $\alpha = 5, \beta = -1$.

The closed form is $a_n = 5 \cdot 2^n - 3^n$, for $n \geq 0$.

Exercise 36.4. $a_2 = 5, a_3 = 13$ and $a_n = 7a_{n-1} - 10a_{n-2}$ for $n \geq 4$.

The characteristic equation is $\chi(x) = x^2 - 7x + 10 = (x - 2)(x - 5)$.

The characteristic roots are $x = 2, 5$.

The general solution is $a_n = \alpha \cdot 2^n + \beta \cdot 5^n$.

The initial values ($n = 2, 3$) produce the linear system of equations

$$4\alpha + 25\beta = 5$$

$$8\alpha + 125\beta = 13$$

The solution to this system is $\alpha = 1, \beta = 1/25$.

The closed form is $a_n = 2^n + \frac{1}{25} \cdot 5^n = 2^n + 5^{n-2}$, for $n \geq 2$.

Exercise 36.5. $a_1 = 3, a_2 = 5$ and $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 3$.

The characteristic equation is $\chi(x) = x^2 - 4x + 4 = (x - 2)^2$.

The characteristic roots are $x = 2, 2$.

The general solution is $a_n = \alpha \cdot 2^n + \beta \cdot n \cdot 2^n$.

The initial values ($n = 1, 2$) produce the linear system of equations

$$2\alpha + 2\beta = 3$$

$$4\alpha + 8\beta = 6$$

The solution to this system is $\alpha = 7/4, \beta = -1/4$.

The closed form is $a_n = \frac{7}{4} \cdot 2^n - \frac{1}{4} \cdot n \cdot 2^n = (7 - n)2^{n-2}$, for $n \geq 1$.

Exercise 36.6. $a_0 = 1, a_1 = 6$ and $a_n = 6a_{n-1} - 9a_{n-2}$ for $n \geq 2$.

The characteristic equation is $\chi(x) = x^2 - 6x + 9 = (x - 3)(x - 3)$.

The characteristic roots are $x = 3, 3$.

The general solution is $a_n = \alpha \cdot 3^n + \beta \cdot n \cdot 3^n$.

The initial values ($n = 0, 1$) produce the linear system of equations

$$\alpha = 1$$

$$3\alpha + 3\beta = 6$$

The solution to this system is $\alpha = 1, \beta = 1$.

The closed form is $a_n = 3^n + n3^n = (1 + n)3^n$, for $n \geq 0$.

Exercise 36.7. $a_1 = 2, a_2 = 8$ and $a_n = a_{n-2}$ for $n \geq 3$.

This one can be solved by inspection, but we may as well go through the motions.

The characteristic equation is $\chi(x) = x^2 - 0x - 1 = (x + 1)(x - 1)$.

The characteristic roots are $x = -1, 1$.

The general solution is $a_n = \alpha(-1)^n + \beta \cdot 1^n$.

The initial values ($n = 1, 2$) produce the linear system of equations

$$-\alpha + \beta = 2$$

$$\alpha + \beta = 8$$

The solution to this system is $\alpha = 3, \beta = 5$.

The closed form is $a_n = 3(-1)^n + 5$, for $n \geq 1$.

Exercise 36.8. $a_0 = 2, a_1 = 5, a_2 = 15$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ for $n \geq 3$.

The characteristic equation is $\chi(x) = x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3)$.

The characteristic roots are $x = 1, 2, 3$.

The general solution is $a_n = \alpha 1^n + \beta \cdot 2^n + \gamma \cdot 3^n$.

The initial values ($n = 0, 1, 2$) produce the linear system of equations

$$\alpha + \beta + \gamma = 2$$

$$\alpha + 2\beta + 3\gamma = 5$$

$$\alpha + 4\beta + 9\gamma = 15$$

The solution to this system is $\alpha = 1, \beta = -1, \gamma = 2$.

The closed form is $a_n = 1 - 2^n + 2 \cdot 3^n$, for $n \geq 0$.

Exercise 36.9. Find a closed form for the terms of the Fibonacci sequence: $f_0 = 0, f_1 = 1$, and for $n \geq 2, f_n = f_{n-1} + f_{n-2}$.

The characteristic equation is $\chi(x) = x^2 - x - 1$.

The characteristic roots are $r_1 = \frac{1+\sqrt{5}}{2}$ and $r_2 = \frac{1-\sqrt{5}}{2}$

The general solution is $a_n = \alpha r_1^n + \beta r_2^n$.

The initial values ($n = 0, 1$) produce the linear system of equations

$$\alpha + \beta = 0$$

$$\alpha r_1 + \beta r_2 = 1$$

The solution to this system is $\alpha = 1/(r_1 - r_2) = 1/\sqrt{5}, \beta = -1/\sqrt{5}$.

The closed form is

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right), \text{ for } n \geq 0.$$

This closed form for the Fibonacci numbers is called Binet's Formula.

Chapter 37 Solutions:

Exercise 37.1. $a_0 = 3, a_1 = 6$ and $a_n = a_{n-1} + 6a_{n-2} + 1$ for $n \geq 2$.

The characteristic equation of the underlying homogeneous relation is

$$\chi(x) = x^2 - x - 6 = (x + 2)(x - 3).$$

The characteristic roots are $x = -2, 3$.

The general homogeneous solution is $a_n^{(h)} = \alpha(-2)^n + \beta \cdot 3^n$.

Since the nonhomogeneous part of the recursion is a constant, our first guess is that the particular solution is of the form $a_n = A$. Substituting that guess into the formula gives

$$A = A + 6A + 1 \text{ with solution } A = -1/6.$$

So the general solution to the nonhomogeneous recursion is

$$a_n = \alpha(-2)^n + \beta 3^n - \frac{1}{6}.$$

The initial values ($n = 0, 1$) produce the linear system of equations

$$\alpha + \beta - \frac{1}{6} = 3$$

$$-2\alpha + 3\beta - \frac{1}{6} = 6$$

The solution to this system is $\alpha = 2/3, \beta = 5/2$.

The closed form is $a_n = \frac{2}{3}(-2)^n + \frac{5}{2} \cdot 3^n - \frac{1}{6}, \text{ for } n \geq 0.$

Exercise 37.2. $a_2 = 5, a_3 = 13$ and $a_n = 7a_{n-1} - 10a_{n-2} + n$ for $n \geq 4$.

The characteristic equation of the underlying homogeneous relation is

$$\chi(x) = x^2 - 7x + 10 = (x - 2)(x - 5).$$

The characteristic roots are $x = 2, 5$.

The general homogeneous solution is $a_n^{(h)} = \alpha 2^n + \beta \cdot 5^n$.

Since the nonhomogeneous part of the recursion is a linear function, our first guess is that the particular solution is of the form $a_n = An + B$. Substituting that guess into the formula gives

$$An + B = 7(A(n - 1) + B) - 10(A(n - 2) + B) + n.$$

Gathering all of the terms on one side of the equation gives

$$(4A - 1)n + (-13A + 4B) = 0.$$

Thus, $4A - 1 = 0$ and $-13A + 4B = 0$. This gives $A = 1/4$ and $B = 13/16$.

So, the general solution to the nonhomogeneous recursion is

$$a_n = \alpha 2^n + \beta 5^n + \frac{n}{4} + \frac{13}{16}.$$

The initial values ($n = 2, 3$) produce the linear system of equations

$$4\alpha + 25\beta + \frac{2}{4} + \frac{13}{16} = 5$$

$$8\alpha + 125\beta + \frac{3}{4} + \frac{13}{16} = 13$$

The solution to this system is $\alpha = 7/12, \beta = 13/240$.

The closed form is $a_n = \frac{7}{12} 2^n + \frac{13}{240} 5^n + \frac{n}{4} + \frac{13}{16} = \frac{7}{3} 2^{n-2} + \frac{13}{48} 5^{n-1} + \frac{n}{4} + \frac{13}{16}$, for $n \geq 2$.

Exercise 37.3. $a_1 = 3, a_2 = 5$ and $a_n = 4a_{n-1} - 4a_{n-2} + 2^n$ for $n \geq 3$.

The characteristic equation of the underlying homogeneous relation is

$$\chi(x) = x^2 - 4x + 4 = (x - 2)(x - 2).$$

The characteristic roots are $x = 2, 2$.

The general homogeneous solution is $a_n^{(h)} = \alpha 2^n + \beta n 2^n$.

Since the nonhomogeneous part of the recursion is an exponential function, our first guess is that the particular solution is of the form $a_n = A 2^n$. Substituting that guess into the formula gives

$$A 2^n = 4A 2^{n-1} - 4A 2^{n-2} + 2^n.$$

Gathering all of the terms involving A on the left side of the equation gives

$$A(2^n - 4 \cdot 2^{n-1} + 4 \cdot 2^{n-2}) = A \cdot 0 = 2^n.$$

Which is impossible.

We might next guess $a_n = An2^n$, but hopefully realize this won't work either. So we guess that $a_n = An^22^n$ may be the correct particular piece. Substitution gives

$$An^22^n = 4A(n-1)^22^{n-1} - 4A(n-2)^22^{n-2} + 2^n.$$

Gathering all of the terms involving A on the left side of the equation gives

$$A2^{n+1} = 2^n \text{ so } A = 1/2.$$

So, the general solution to the nonhomogeneous recursion is

$$a_n = \alpha 2^n + \beta n 2^n + \frac{1}{2} n^2 2^n = \alpha 2^n + \beta n 2^n + n^2 2^{n-1}.$$

The initial values ($n = 1, 2$) produce the linear system of equations

$$2\alpha + 2\beta + 1 = 3$$

$$4\alpha + 8\beta + 8 = 5$$

The solution to this system is $\alpha = 11/4, \beta = -7/4$.

The closed form is $a_n = \frac{11}{4} 2^n - \frac{7}{4} n 2^n + n^2 2^{n-1} = (11 - 7n + 2n^2) 2^{n-2}$, for $n \geq 1$.

Exercise 37.4. $a_0 = 1, a_1 = 6$ and $a_n = 6a_{n-1} - 9a_{n-2} + n$ for $n \geq 2$.

The characteristic equation of the underlying homogeneous relation is

$$\chi(x) = x^2 - 6x + 9 = (x - 3)(x - 3).$$

The characteristic roots are $x = 3, 3$.

The general homogeneous solution is $a_n^{(h)} = \alpha 3^n + \beta n 3^n$.

Since the nonhomogeneous part of the recursion is a linear function, our first guess is that the particular solution is of the form $a_n = An + B$. Substituting that guess into the formula gives

$$An + B = 6(A(n-1) + B) - 9(A(n-2) + B) + n.$$

Gathering all of the terms on the left side of the equation gives

$$(4A - 1)n + (4B - 12A) = 0. \text{ which means } A = \frac{1}{4} \text{ and } B = \frac{3}{4}.$$

So, the general solution to the nonhomogeneous recursion is

$$a_n = \alpha 3^n + \beta n 3^n + \frac{n}{4} + \frac{3}{4}.$$

The initial values ($n = 0, 1$) produce the linear system of equations

$$2\alpha + \frac{3}{4} = 1$$

$$3\alpha + 3\beta + 1 = 6$$

The solution to this system is $\alpha = 1/4, \beta = 17/12$.

The closed form is $a_n = \frac{1}{4}3^n + \frac{17}{4}n3^{n-1} + \frac{n}{4} + \frac{3}{4}$, for $n \geq 0$.

Exercise 37.5. $a_0 = 2, a_1 = 5$ and $a_2 = 15$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3} + 2n + 1$ for $n \geq 3$.

The characteristic equation of the underlying homogeneous relation is

$$\chi(x) = x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3).$$

The characteristic roots are $x = 1, 2, 3$.

The general homogeneous solution is $a_n^{(h)} = \alpha 2^n + \beta 2^n + \gamma 3^n$.

Since the nonhomogeneous part of the recursion is a linear function, our first guess is that the particular solution is of the form $a_n = An + B$. Substituting that guess into the formula gives

$$An + B = 6(A(n - 1) + B) - 11(A(n - 2) + B) + 6(A(n - 3) + B) + 2n + 1.$$

Gathering all of the terms involving A on the left side of the equation gives

$$-2n + (2A - 1) = 0$$

Which is impossible.

Our next guess is $a_n = An^2 + Bn$. After substitution and gathering terms we get

$$(4A - 2)n + (2B - 16A + 1) = 0 \text{ which means } A = 1/2 \text{ and } B = 9/2.$$

So, the general solution to the nonhomogeneous recursion is

$$a_n = \alpha + \beta 2^n + \gamma 3^n + \frac{n^2}{2} + \frac{9n}{2}.$$

The initial values ($n = 0, 1, 2$) produce the linear system of equations

$$\alpha + \beta + \gamma = 2$$

$$\alpha + 2\beta + 3\gamma + 5 = 5$$

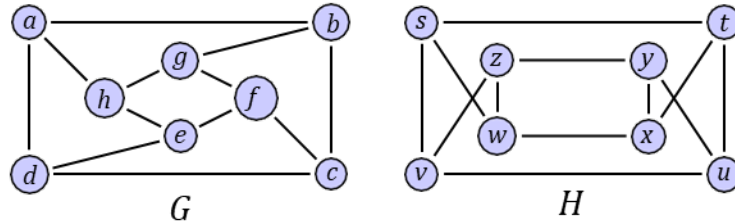
$$\alpha + 4\beta + 9\gamma + 10 = 15$$

The solution to this system is $\alpha = 8, \beta = -10, \gamma = 4$.

The closed form is $a_n = 8 - 10 \cdot 2^n + 4 \cdot 3^n + \frac{n^2}{2} + \frac{9n}{2}$, for $n \geq 0$.

Chapter 38 Solutions:

Exercise 38.1. Find a graph isomorphism $\varphi: G \rightarrow H$. Verify the adjacency-preserving property by showing that the adjacency matrices A_G and A_H^φ are identical.



There are many isomorphisms. One is

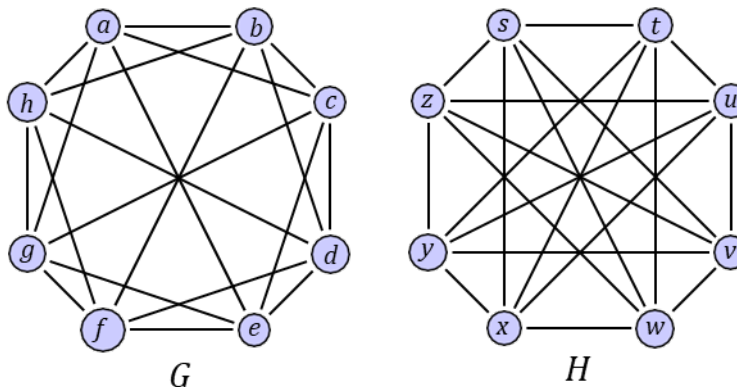
$$\begin{aligned} a &\rightarrow s & b &\rightarrow t & c &\rightarrow u & d &\rightarrow v \\ e &\rightarrow z & f &\rightarrow y & g &\rightarrow x & h &\rightarrow w \end{aligned}$$

The adjacency matrix for G using the vertex ordering a, b, c, d, e, f, g, h is

$$A_G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} = A_H^\varphi$$

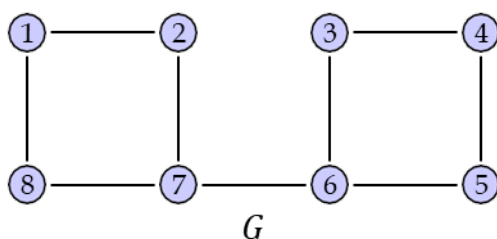
The matrix A_H^φ is the adjacency matrix of H using the ordering s, t, u, v, z, y, x, w .

Exercise 38.2. Prove that the graphs G and H are not isomorphic.

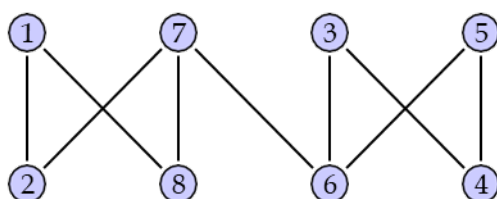


Let $\bar{G}$ and $\bar{H}$ denote the edge-wise complements of G and H with respect to the complete graph K_8 . It is clear that if G and H are isomorphic, then so are $\bar{G}$ and $\bar{H}$. But $\bar{G}$ is just an 8-cycle, while $\bar{H}$ is the disjoint union of two 4-cycles. So $\bar{G}$ and $\bar{H}$ are not isomorphic. Therefore neither are G and H .

Exercise 38.3. Redraw the graph G as a bipartite graph.

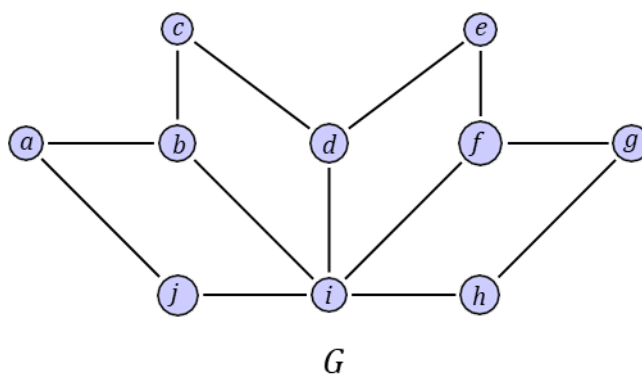


There are several possible solutions. One is



Chapter 39 Solutions:

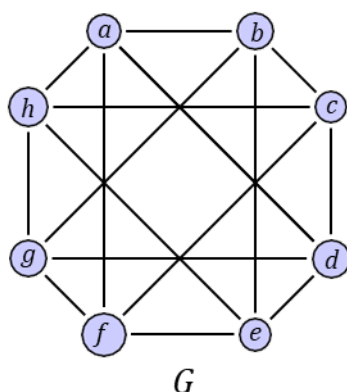
Exercise 39.1. Give a Hamiltonian cycle as a list of vertices for the graph G . Explain why G does not have an Eulerian cycle.



A Hamiltonian cycle is $a, b, c, d, e, f, g, h, i, j, a$ – just the outer rim.

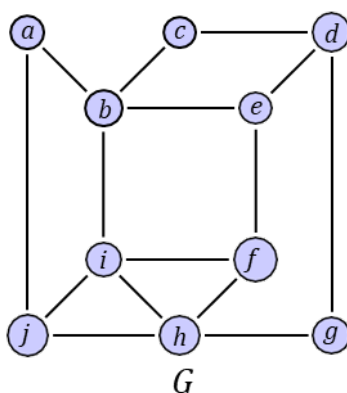
The graph has four vertices of odd degree (b, d, f, i) so it is not Eulerian.

Exercise 39.2. Find an Eulerian cycle for the graph G as a list of vertices.



An Eulerian cycle is $a, b, c, d, e, f, g, h, a, d, g, b, e, h, c, f, a$.

Exercise 39.3. Prove that the graph G has no Hamiltonian cycle.



In a Hamiltonian cycle, exactly two edges must be used at each vertex. Therefore, a Hamiltonian cycle would include the edges $\{a, b\}$, $\{a, j\}$, $\{b, c\}$, $\{c, d\}$, $\{d, g\}$, and $\{g, h\}$. But then the edges $\{b, i\}$, $\{b, e\}$, and $\{e, d\}$ would be forbidden. This leaves only the single edge $\{e, f\}$ to include e in the cycle. Conclusion: the graph G is not Hamiltonian.

GNU Free Documentation License

Appendix: GNU Free Documentation

License Version 1.2, November 2002

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

B.1 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. Secondly, 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:

- (1) 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.
- (2) 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.
- (3) C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- (4) D. Preserve all the copyright notices of the Document.
- (5) E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- (6) 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.
- (7) G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- (8) H. Include an unaltered copy of this License.
- (9) 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.
- (10) 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.
- (11) 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.
- (12) 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.
- (13) M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- (14) N. Do not re-title any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- (15) 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.